Social Engineering

Module 09

Social Engineering

Social engineering is the art of convincing users to reveal confidential information.

Lab Scenario

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Organizations fall victim to social engineering tactics despite having strong security policies and solutions in place. This is because social engineering exploits the most vulnerable link in information system security—employees. Cybercriminals are increasingly using social engineering techniques to target people's weaknesses or play on their good natures.

Social engineering can take many forms, including phishing emails, fake sites, and impersonation. If the features of these techniques make them an art, the psychological insights that inform them make them a science.

While non-existent or inadequate defense mechanisms in an organization can encourage attackers to use various social engineering techniques to target its employees, the bottom line is that there is no technological defense against social engineering. Organizations must educate employees on how to recognize and respond to these attacks, but only constant vigilance will minimize attackers' chances of success.

As an expert ethical hacker and penetration tester, you need to assess the preparedness of your organization or the target of evaluation against social engineering attacks. It is important to note, however, that social engineering primarily requires soft skills. The labs in this module therefore demonstrate several techniques that facilitate or automate certain facets of social engineering attacks.

Lab Objectives

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 09 Social Engineering

The objective of the lab is to use social engineering and related techniques to:

- Sniff user/employee credentials such as employee IDs, names, and email addresses
- Obtain employees' basic personal details and organizational information
- Obtain usernames and passwords
- Perform phishing
- Detect phishing

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 45 Minutes

Overview of Social Engineering

Social engineering is the art of manipulating people to divulge sensitive information that will be used to perform some kind of malicious action. Because social engineering targets human weakness, even organizations with strong security policies are vulnerable to being compromised by attackers. The impact of social engineering attacks on organizations can include economic losses, damage to goodwill, loss of privacy, risk of terrorism, lawsuits and arbitration, and temporary or permanent closure.

There are many ways in which companies may be vulnerable to social engineering attacks. These include:

- Insufficient security training
- Unregulated access to information
- An organizational structure consisting of several units
- Non-existent or lacking security policies

Lab Tasks

Ethical hackers or penetration testers use numerous tools and techniques to perform social engineering tests. The recommended labs that will assist you in learning various social engineering techniques are:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform Social Engineering using Various Techniques	√	√	√
	1.1 Sniff Users' Credentials using the Social-Engineer Toolkit (SET)	√		√
	1.2 Perform Phishing using ShellPhish		√	√
2	Detect a Phishing Attack	√	√	√
	2.1 Detect Phishing using Netcraft	√		√
	2.2 Detect Phishing using PhishTank		√	√
3	Audit Organization's Security for Phishing Attacks	√		√
	3.1 Audit Organization's Security for Phishing Attacks using OhPhish	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab
1

Perform Social Engineering using Various Techniques

Social engineering techniques are used to gather sensitive information from people or organizations in order to commit fraud or carry out other criminal activities.

ICON KEY

🗀 Valuable Information

✎ Test Your Knowledge

💻 Web Exercise

📖 Workbook Review

Lab Scenario

As a professional ethical hacker or penetration tester, you should use various social engineering techniques to examine the security of an organization and the awareness of employees.

In a social engineering test, you should try to trick the user into disclosing personal information such as credit card numbers, bank account details, telephone numbers, or confidential information about their organization or computer system. In the real world, attackers would use these details either to commit fraud or to launch further attacks on the target system.

Lab Objectives

🗀 **Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 09 Social Engineering**

- Sniff users' credentials using the Social-Engineer Toolkit (SET)
- Perform phishing using ShellPhish

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Overview of Social Engineering Techniques

There are three types of social engineering attacks: human-, computer-, and mobile-based.

- **Human-based social engineering** uses interaction to gather sensitive information, employing techniques such as impersonation, vishing, and eavesdropping
- **Computer-based social engineering** uses computers to extract sensitive information, employing techniques such as phishing, spamming, and instant messaging
- **Mobile-based social engineering** uses mobile applications to obtain information, employing techniques such as publishing malicious apps, repackaging legitimate apps, using fake security applications, and SMiShing (SMS Phishing)

Lab Tasks

TASK 1

Sniff Users' Credentials using the Social-Engineer Toolkit (SET)

As an ethical hacker, penetration tester, or security administrator, you should be familiar with SET and be able to use it to perform various tests for network vulnerabilities.

Here, we will sniff credentials using the SET.

The Social-Engineer Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing via social engineering. SET is particularly useful to attackers, because it is freely available and can be used to carry out a range of attacks.

1. Turn on the **Windows 10**, **Windows Server 2019**, **Parrot Security** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

TASK 1.1

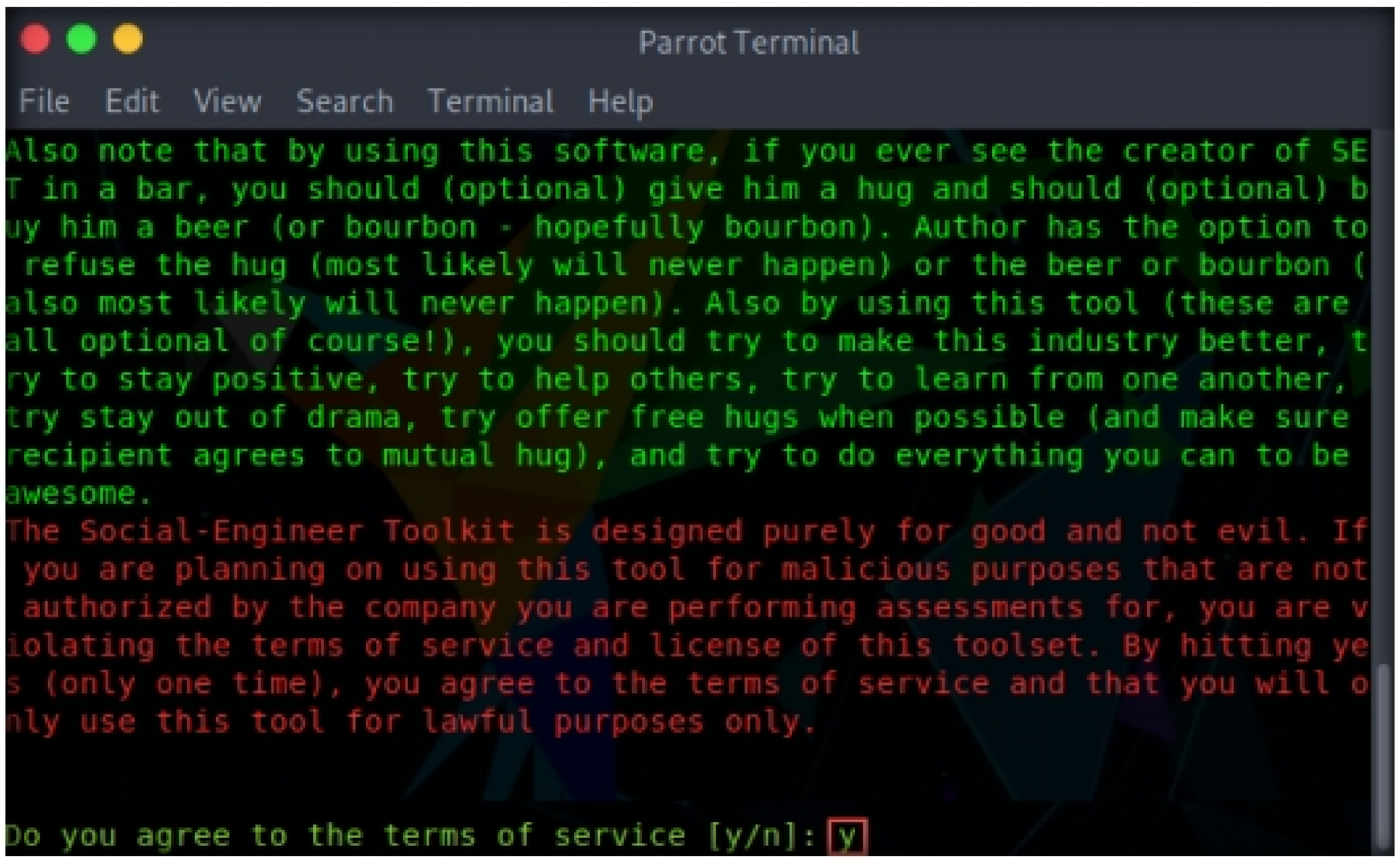
Launch Social Engineering Toolkit (SET)

3. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Exploitation Tools → Social Engineering → social engineering toolkit**.
4. A **Terminal window** appears, in the **[sudo] password for attacker** field, type **toor** and press **Enter**.

Note: The password that you type will not be visible.

5. In the terminal window, the information about **Social-Engineer Toolkit** appears.

6. Type **y** and press **Enter** to agree to the terms of services.



```
Also note that by using this software, if you ever see the creator of SE
T in a bar, you should (optional) give him a hug and should (optional) b
uy him a beer (or bourbon - hopefully bourbon). Author has the option to
 refuse the hug (most likely will never happen) or the beer or bourbon (
also most likely will never happen). Also by using this tool (these are
all optional of course!), you should try to make this industry better, t
ry to stay positive, try to help others, try to learn from one another,
try stay out of drama, try offer free hugs when possible (and make sure
recipient agrees to mutual hug), and try to do everything you can to be
awesome.
The Social-Engineer Toolkit is designed purely for good and not evil. If
 you are planning on using this tool for malicious purposes that are not
 authorized by the company you are performing assessments for, you are v
iolating the terms of service and license of this toolset. By hitting ye
s (only one time), you agree to the terms of service and that you will o
nly use this tool for lawful purposes only.


Do you agree to the terms of service [y/n]: y
```

Figure 1.1.1: Agreeing to the terms of service

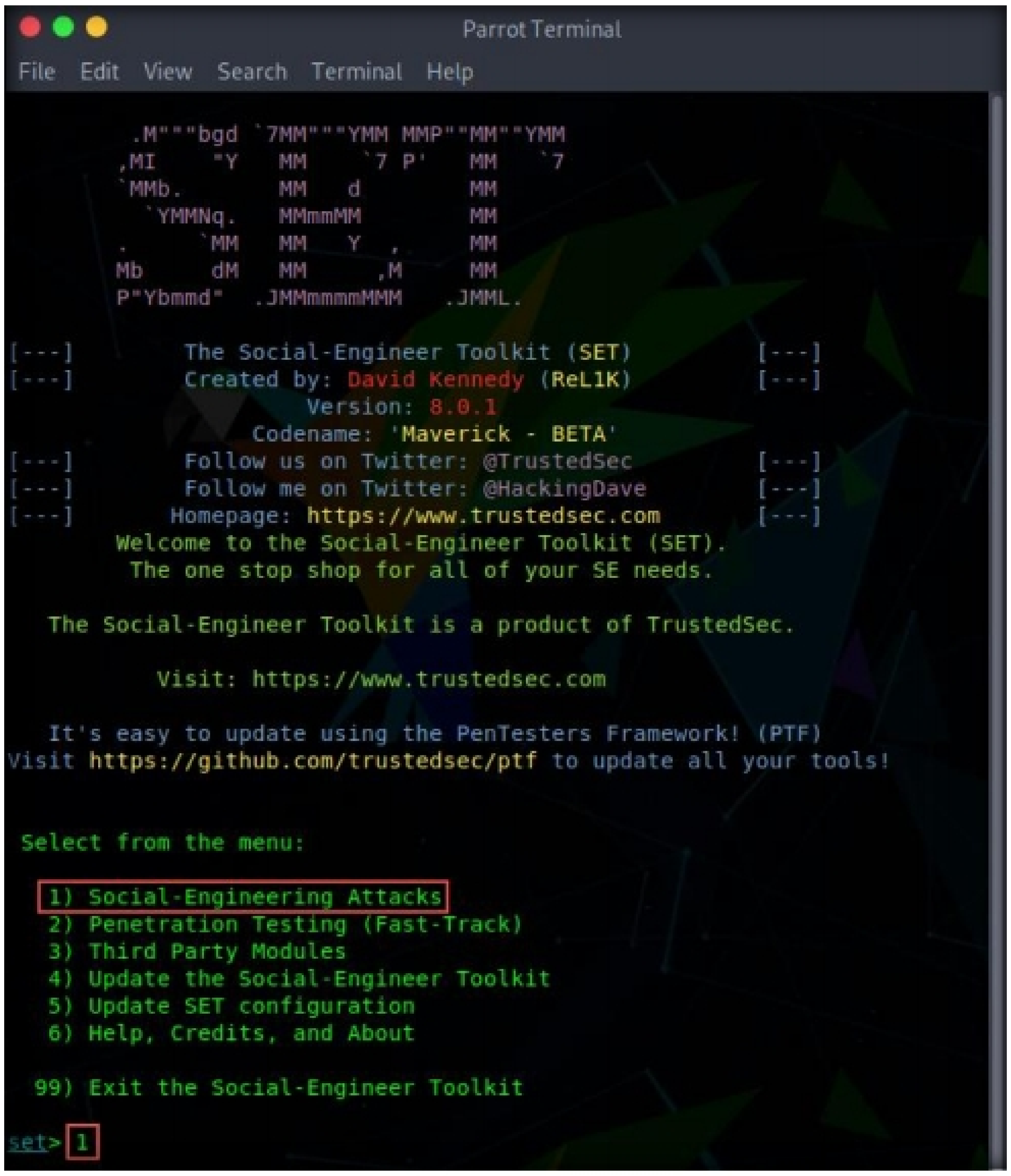
The Social-Engineer Toolkit (SET) allows attackers to draft email messages, attach malicious files, and send them to a large number of people using spear phishing. Moreover, SET's multi-attack method allows Java applets, the Metasploit browser, and Credential Harvester/Tabnabbing to be used simultaneously. SET categorizes attacks according to the attack vector used such as email, web, and USB.

TASK 1.2

Create a Cloned Website

7. The **SET** menu appears, as shown in the screenshot. Type **1** and press **Enter** to choose **Social-Engineering Attacks**.

Note: The version of the tool might differ in your lab environment.

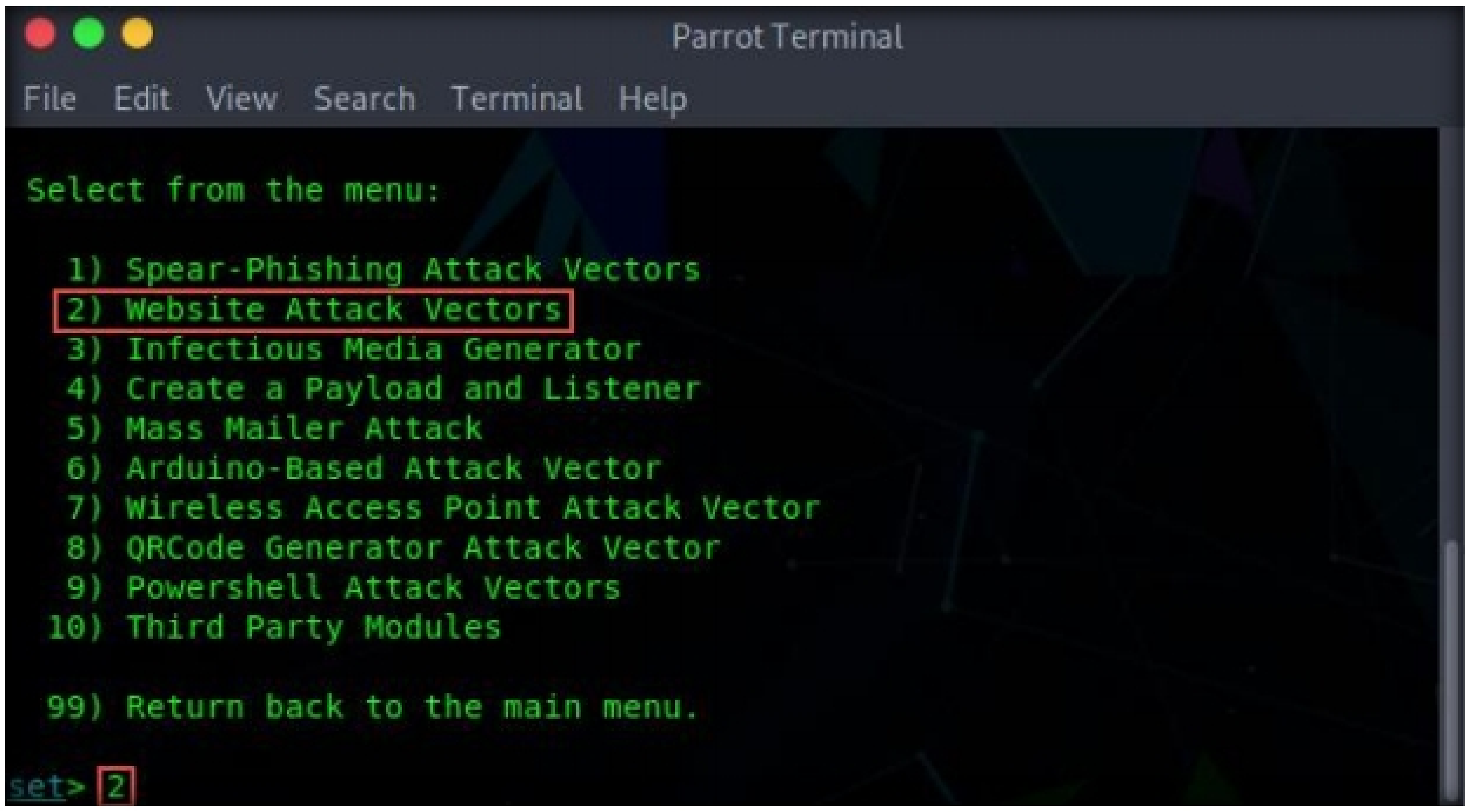


```
          .M"""bgd `7MM"""YMM MMP""MM""YMM
         ,MI    "Y   MM    `7 P'   MM   `7
         `MMb.       MM   d        MM
           `YMMNq.   MMmmMM        MM
         .     `MM   MM   Y  ,     MM
         Mb     dM   MM     ,M     MM
         P"Ybmmd"  .JMMmmmmMMM   .JMML.

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.1
                  Codename: 'Maverick - BETA'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
         Welcome to the Social-Engineer Toolkit (SET).
          The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 1
```

Figure 1.1.2: The SET main menu

Although many kinds of attacks can be carried out using SET, it is also a must-have tool for penetration testers to check for vulnerabilities. For this reason, SET is the standard for social engineering penetration tests, and is strongly supported within the security community.

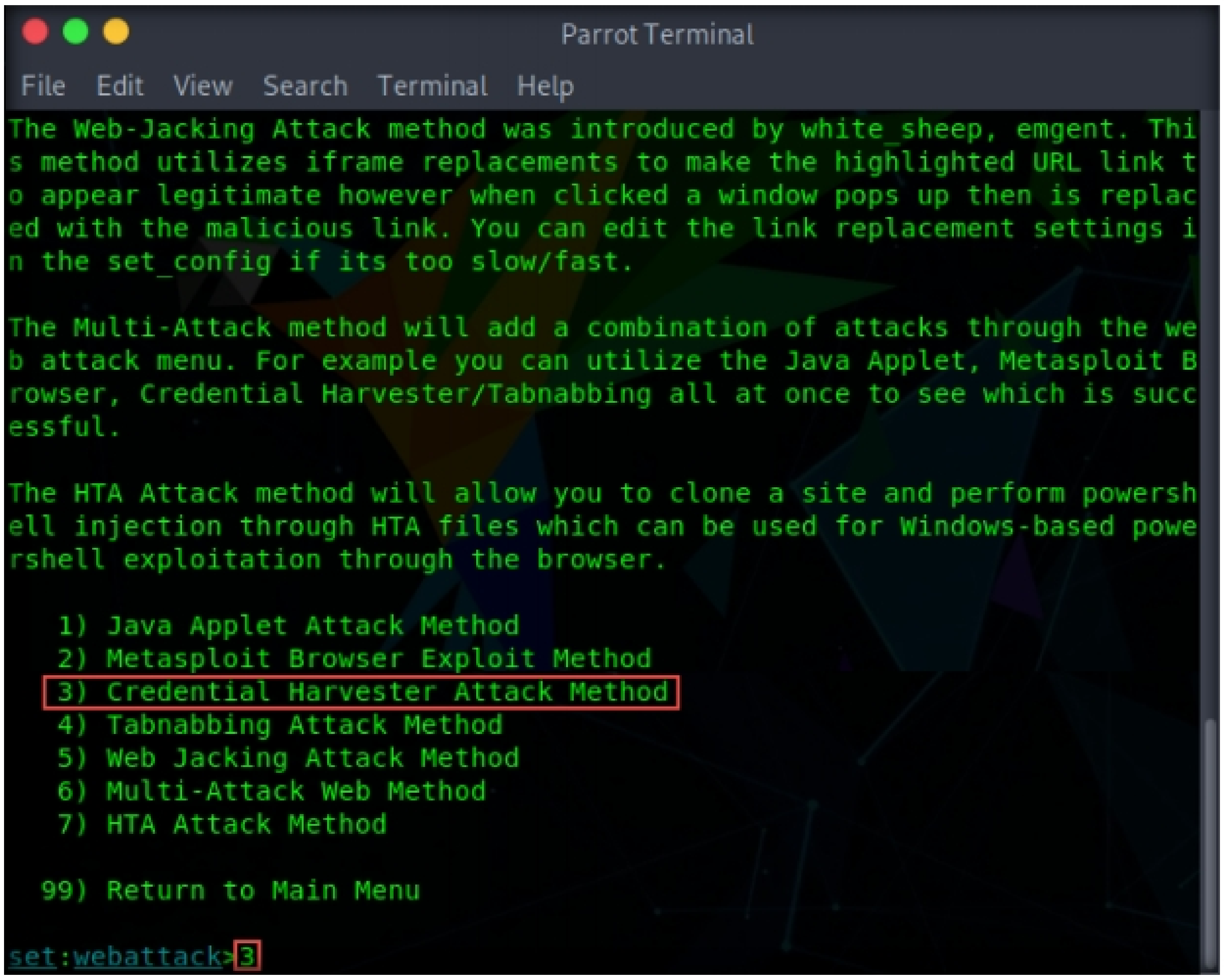
8. A list of options for **Social-Engineering Attacks** appears; type **2** and press **Enter** to choose **Website Attack Vectors**.



```
Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) Wireless Access Point Attack Vector
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) Third Party Modules

 99) Return back to the main menu.

set> 2
```

Figure 1.1.3: Choosing Website Attack Vectors

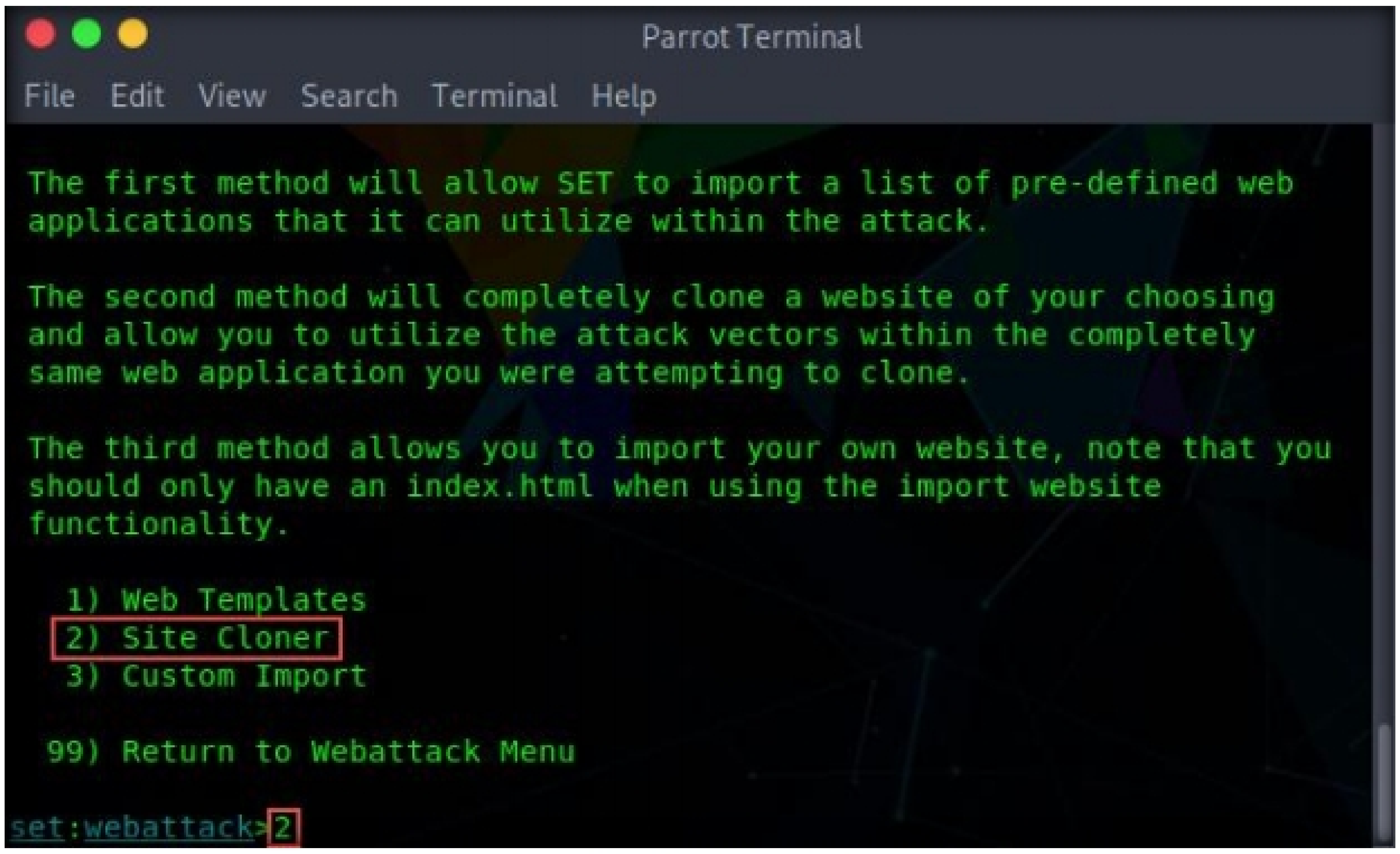
9. A list of options in **Website Attack Vectors** appears; type **3** and press **Enter** to choose **Credential Harvester Attack Method**.



```
The Web-Jacking Attack method was introduced by white_sheep, emgent. Thi
s method utilizes iframe replacements to make the highlighted URL link t
o appear legitimate however when clicked a window pops up then is replac
ed with the malicious link. You can edit the link replacement settings i
n the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the we
b attack menu. For example you can utilize the Java Applet, Metasploit B
rowser, Credential Harvester/Tabnabbing all at once to see which is succ
essful.

The HTA Attack method will allow you to clone a site and perform powersh
ell injection through HTA files which can be used for Windows-based powe
rshell exploitation through the browser.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

Figure 1.1.4: Choosing the Credential Harvester Attack Method

10. Type **2** and press **Enter** to choose **Site Cloner** from the menu.



```
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

  1) Web Templates
  2) Site Cloner
  3) Custom Import

 99) Return to Webattack Menu

set:webattack>2
```

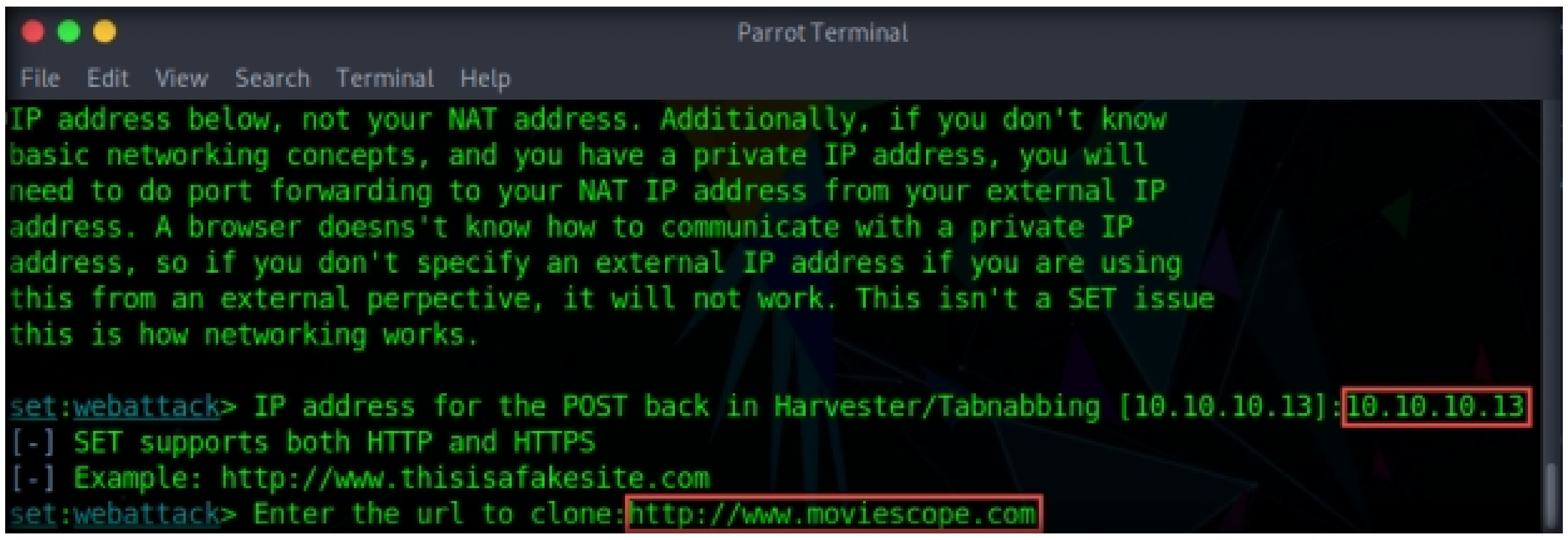
Figure 1.1.5: Choosing Site Cloner

11. Type the IP address of the local machine (**10.10.10.13**) in the prompt for "**IP address for the POST back in Harvester/Tabnabbing**" and press **Enter**.

Note: In this case, we are targeting the **Parrot Security** virtual machine (IP address: **10.10.10.13**). These details may vary in your lab environment.

12. Now, you will be prompted for the URL to be cloned; type the desired URL in "**Enter the url to clone**" and press **Enter**. In this task, we will clone the URL **https://www.moviescope.com**.

Note: You can clone any URL of your choice.

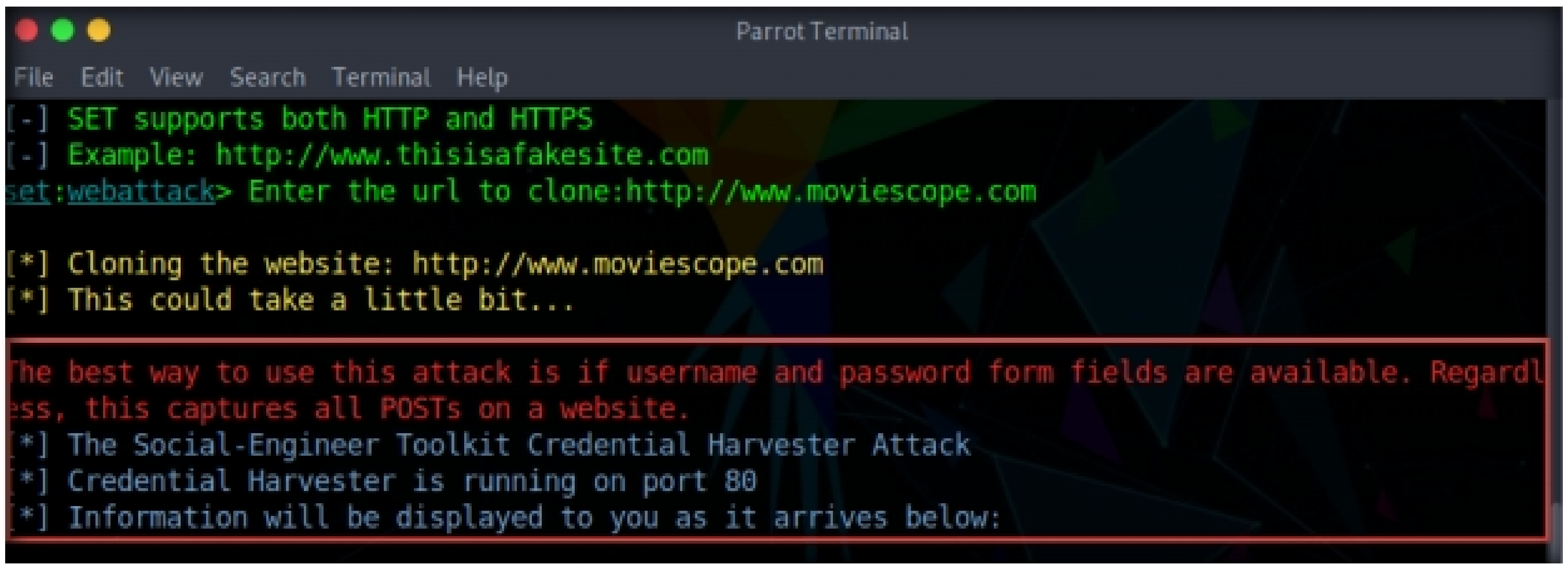


```
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.10.13]:10.10.10.13
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.moviescope.com
```

Figure 1.1.6: Providing URL to be cloned

13. If a message appears that reads **Press {return} if you understand what we're saying here**, press **Enter**.

14. After cloning is completed, a highlighted message appears. The credential harvester initiates, as shown in the screenshot.



```
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.moviescope.com

[*] Cloning the website: http://www.moviescope.com
[*] This could take a little bit...

he best way to use this attack is if username and password form fields are available. Regardl
ss, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Figure 1.1.7: SET Website Cloning

TASK 1.3

Create and Send a Crafted Email

15. Having successfully cloned a website, you must now send the IP address of your **Parrot Security** machine to a victim and try to trick him/her into clicking on the link.

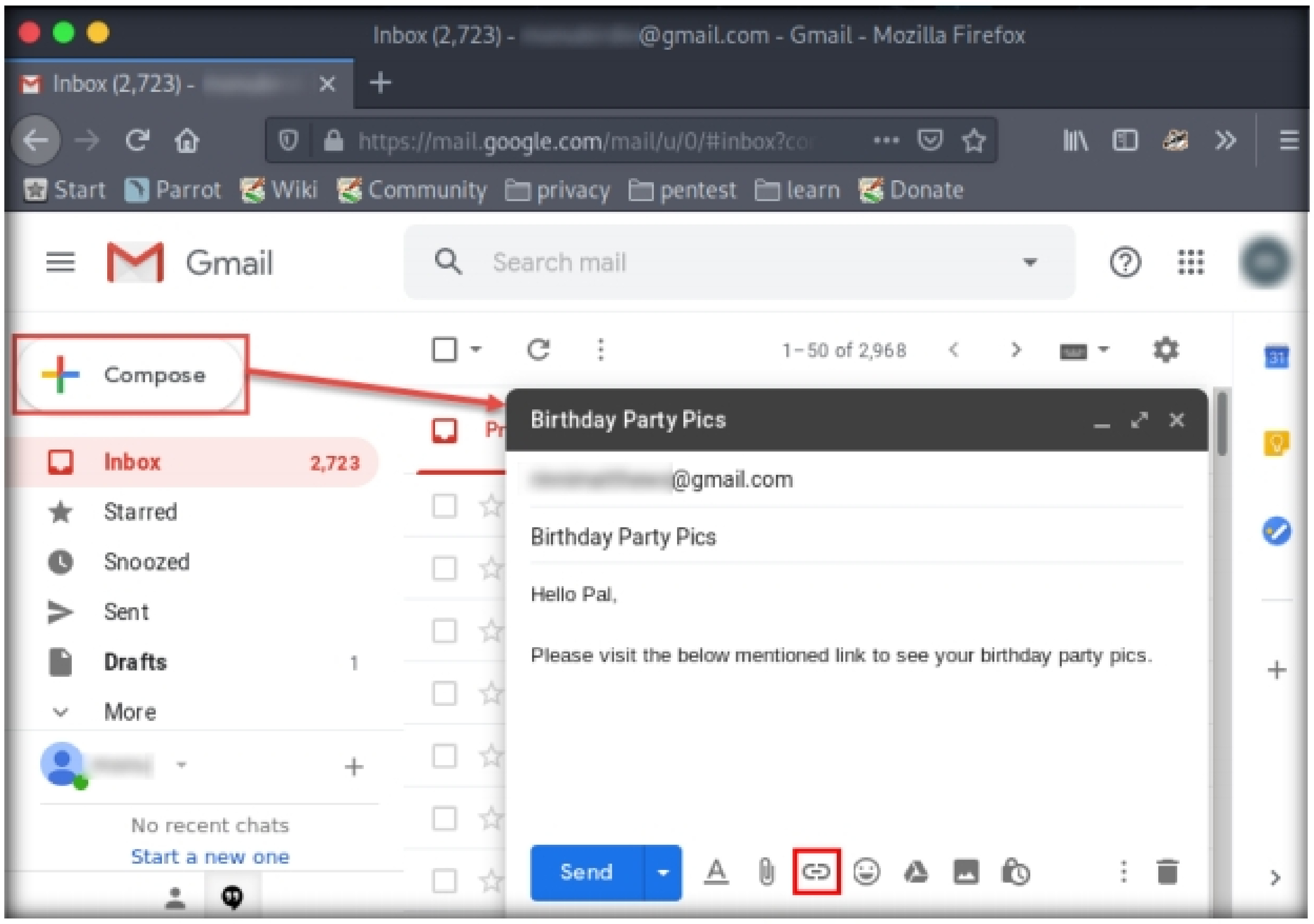
16. Launch a web browser window and open your email account (in this example, we are using **Mozilla Firefox** and **Gmail**, respectively). Log in, and compose an email.

Note: You can log in to any email account of your choice.

17. After logging into your email account, click the **Compose** button in the left pane and compose a fake but enticing email to lure a user into opening the email and clicking on a malicious link.

Note: A good way to conceal a malicious link in a message is to insert text that looks like a legitimate MovieScope URL (in this case), but that actually links to your malicious cloned MovieScope page.

18. Position the cursor where you wish to place the fake URL, then click the **Insert link** icon (🔗).



Inbox (2,723) - [redacted]@gmail.com - Gmail - Mozilla Firefox

Birthday Party Pics

[redacted]@gmail.com

Birthday Party Pics

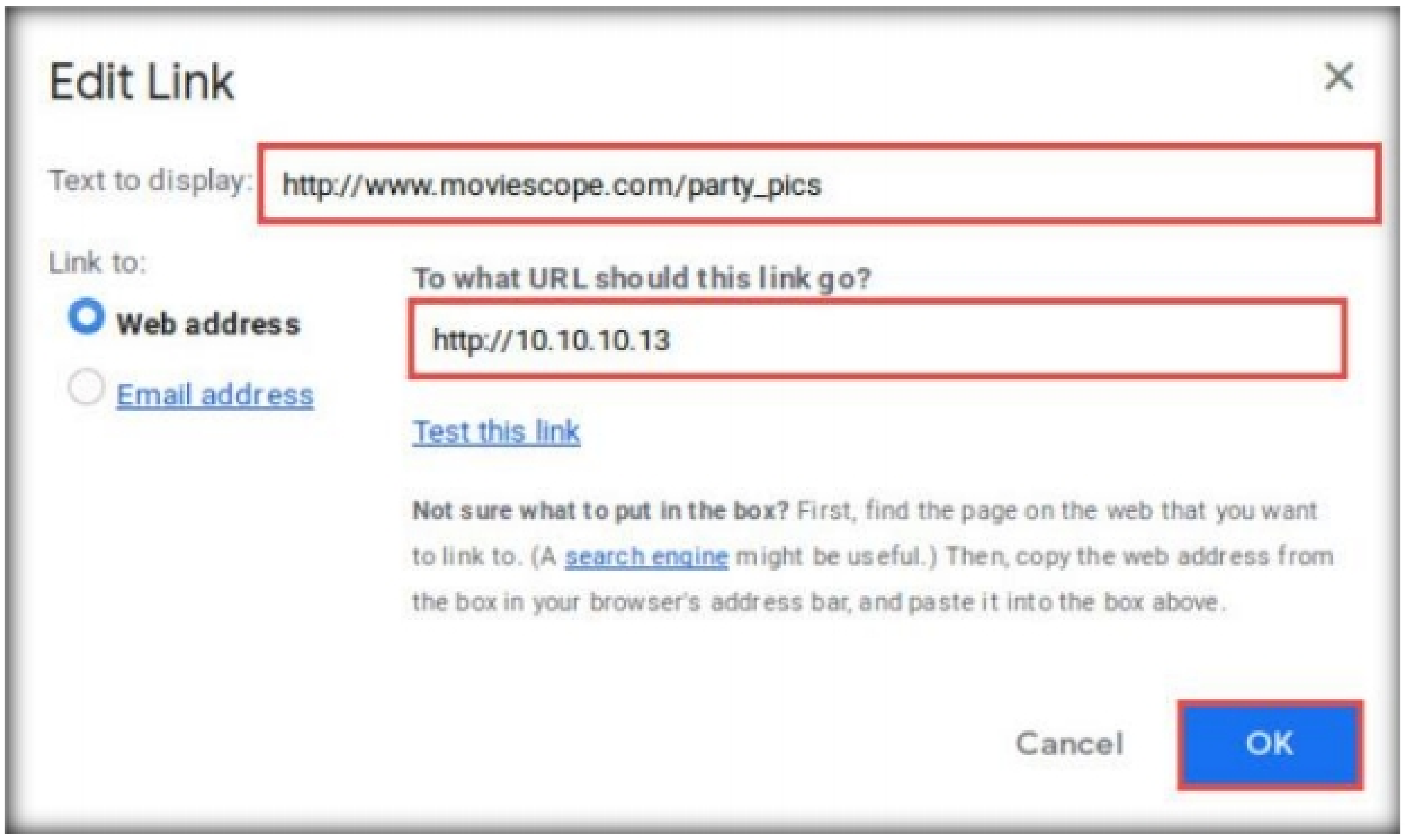
Hello Pal,

Please visit the below mentioned link to see your birthday party pics.

https://mail.google.com/mail/u/0/#inbox?c
Start
Parrot
Wiki
Community
privacy
pentest
learn
Donate
Gmail
Search mail
Compose
1–50 of 2,968
Inbox 2,723
Starred
Snoozed
Sent
Drafts 1
More
No recent chats
Start a new one
Send

Figure 1.1.8: Creating and concealing a malicious link

19. In the **Edit Link** window, first type the actual address of your cloned site in the **Web address** field under the **Link to** section. Then, type the fake URL in the **Text to display** field. In this case, the actual address of our cloned MovieScope site is **http://10.10.10.13**, and the text that will be displayed in the message is **http://www.moviescope.com/party_pics**; click **OK**.



Edit Link

Text to display: http://www.moviescope.com/party_pics

Link to:

● Web address

○ Email address

To what URL should this link go?

http://10.10.10.13

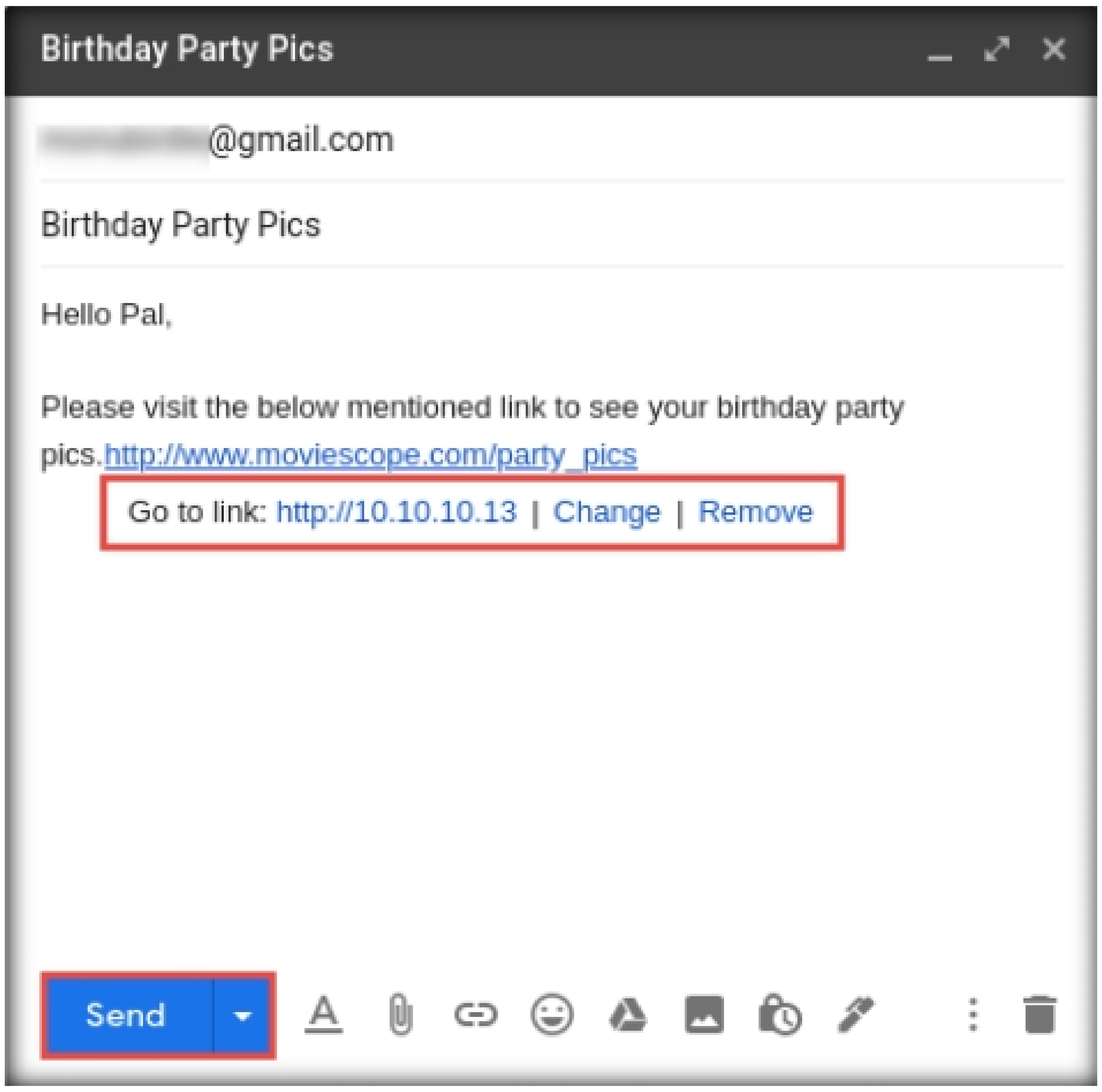
Test this link

Not sure what to put in the box? First, find the page on the web that you want to link to. (A search engine might be useful.) Then, copy the web address from the box in your browser's address bar, and paste it into the box above.

Figure 1.1.9: The Edit Link window

20. The fake URL should appear in the message body, as shown in the screenshot.

21. Verify that the fake URL is linked to the correct cloned site: in Gmail, click the link; the actual URL will be displayed in a "**Go to link**" pop-up. Once verified, send the email to the intended user.



Birthday Party Pics

@gmail.com

Birthday Party Pics

Hello Pal,

Please visit the below mentioned link to see your birthday party pics.http://www.moviescope.com/party_pics

Go to link: http://10.10.10.13 | Change | Remove

Send

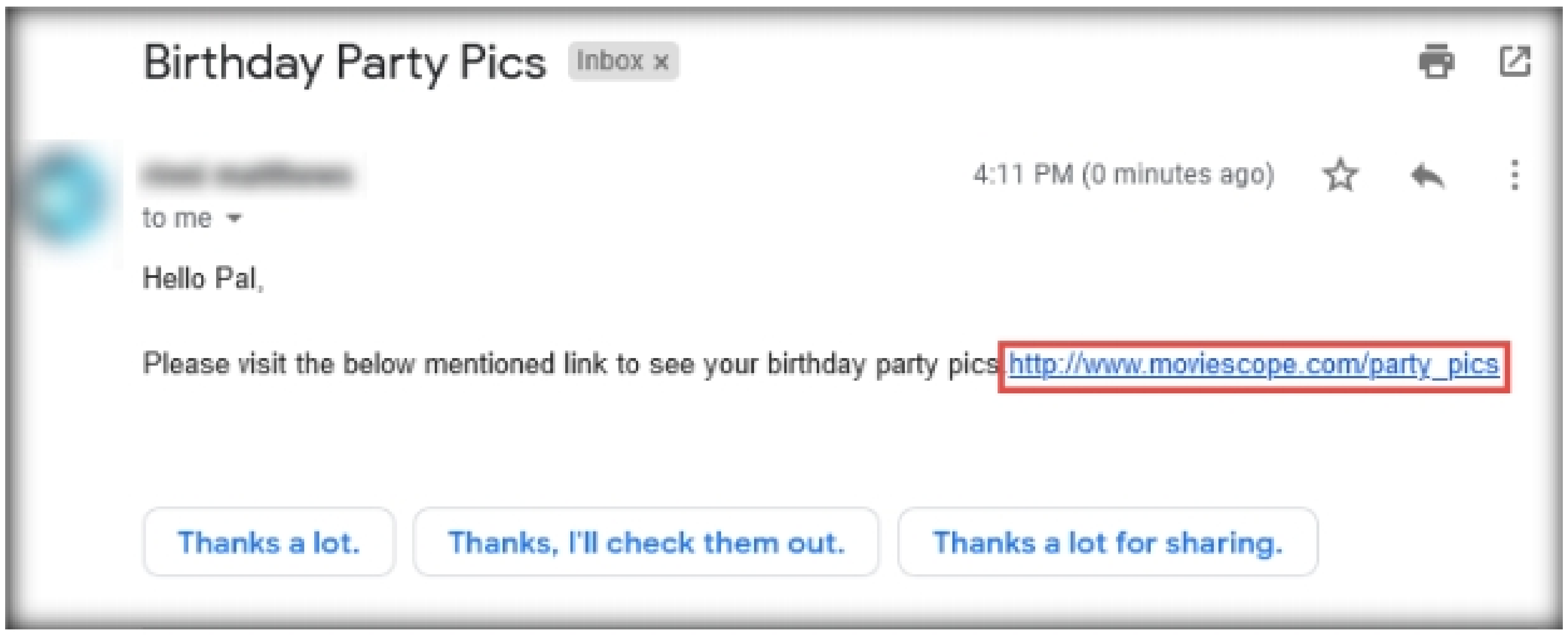
Figure 1.1.10: The cloned site URL hidden in a fake URL

TASK 1.4

Open the Phishing Email and Log in to the Cloned Website

22. Switch to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

23. Open any web browser (in this example, we are using **Mozilla Firefox**), sign in to the email account to which you sent the phishing mail as an attacker. Open the email you sent previously and click to open the malicious link.



Birthday Party Pics
Inbox ×
4:11 PM (0 minutes ago)
to me

Hello Pal,

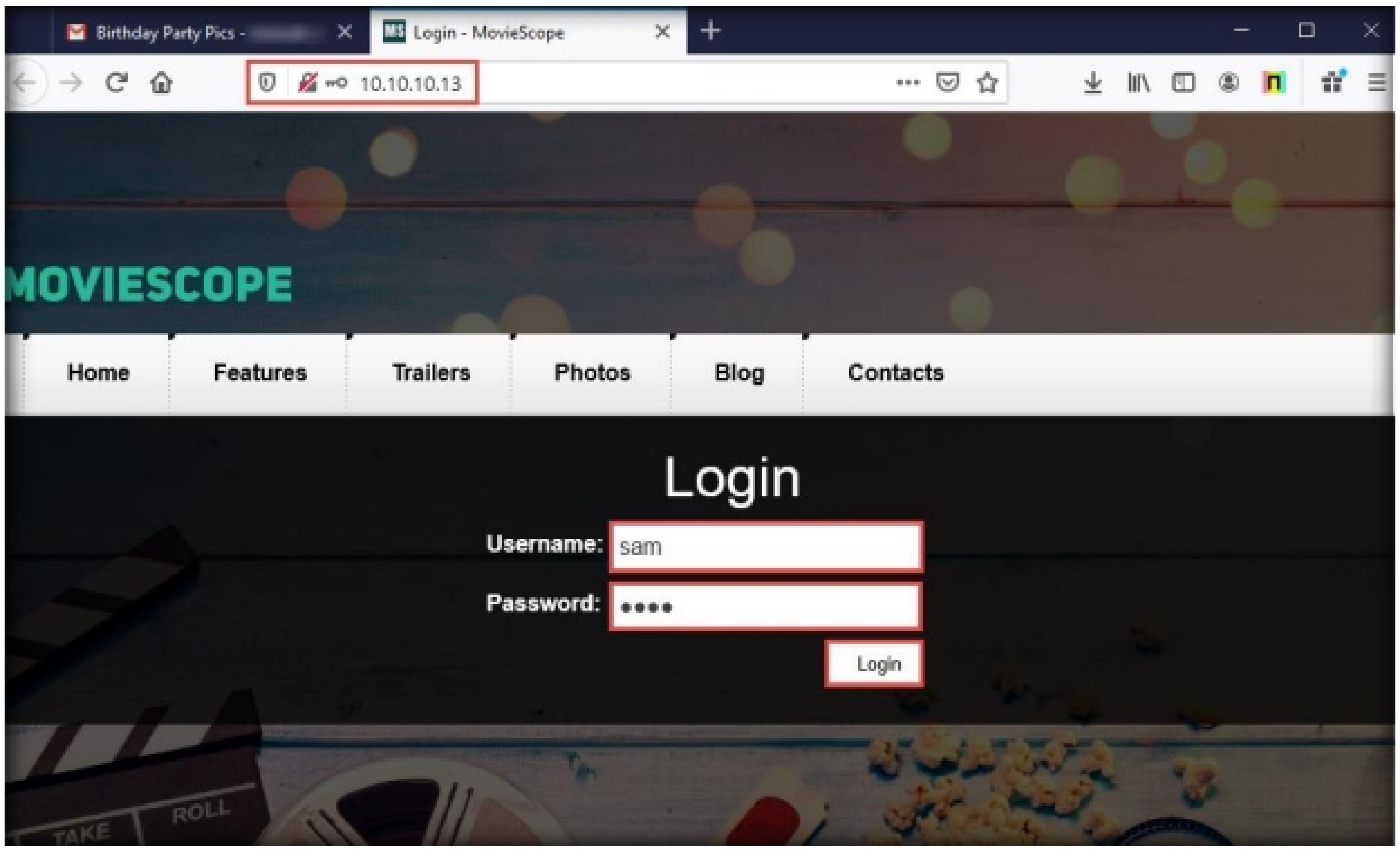
Please visit the below mentioned link to see your birthday party pics http://www.moviescope.com/party_pics

Thanks a lot.
Thanks, I'll check them out.
Thanks a lot for sharing.

Figure 1.1.11: Phishing email

24. When the victim (you in this case) clicks the URL, a new tab opens up, and he/she will be presented with a replica of **www.moviescope.com**.

25. The victim will be prompted to enter his/her username and password into the form fields, which appear as they do on the genuine website. When the victim enters the **Username** and **Password** and clicks **Login**, he/she will be redirected to the legitimate **MovieScope** login page. Note the different URLs in the browser address bar for the cloned and real sites.


Birthday Party Pics - [redacted]
Login - MovieScope
10.10.10.13
MOVIESCOPE
Home
Features
Trailers
Photos
Blog
Contacts
Login
Login

Username: sam

Password: ●●●●

Figure 1.1.12: Fake MovieScope login page

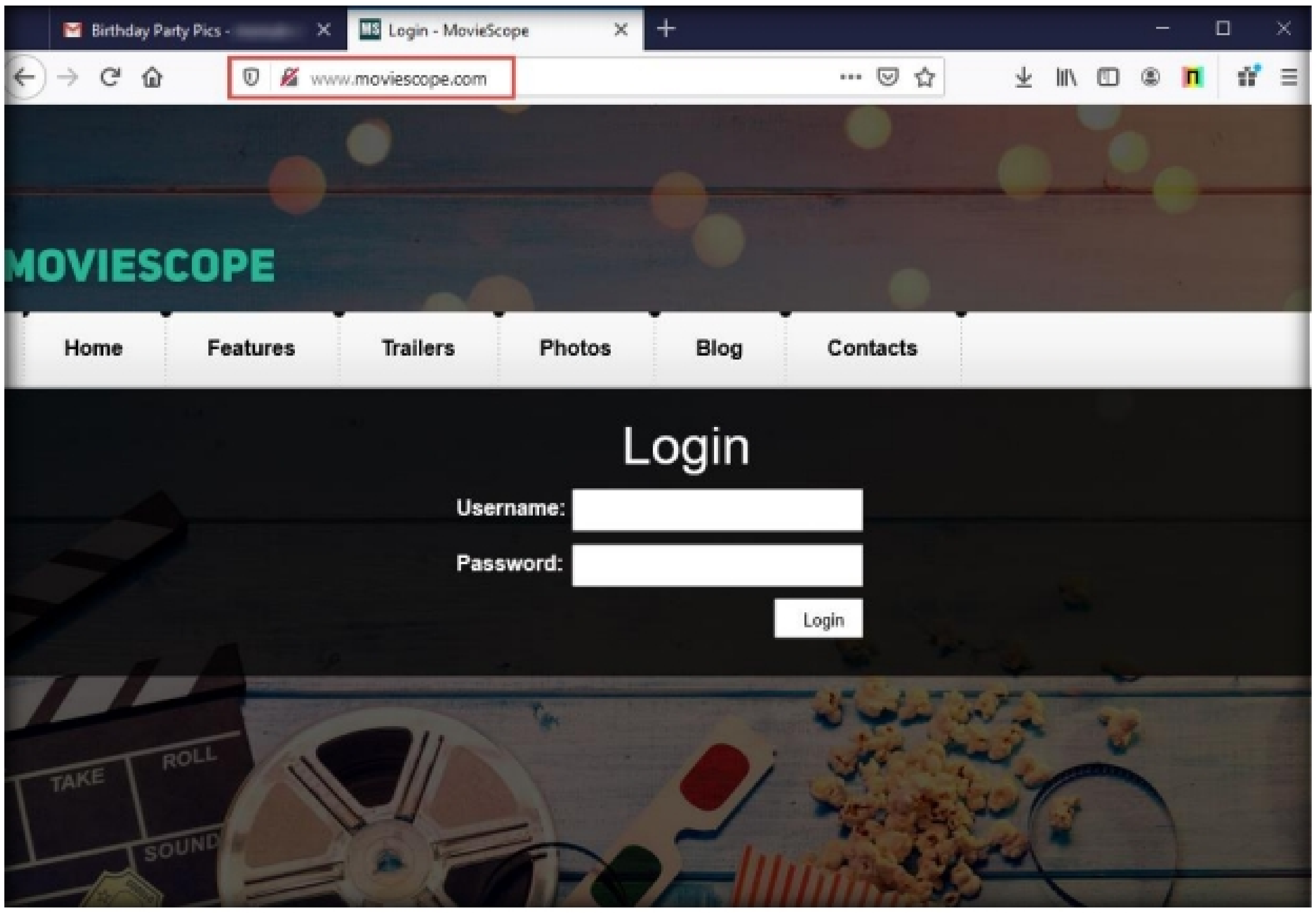

Birthday Party Pics - [redacted]
Login - MovieScope
www.moviescope.com
MOVIESCOPE
Home
Features
Trailers
Photos
Blog
Contacts
Login
Username:
Password:
Login
TAKE
ROLL
SOUND

Figure 1.1.13: Legitimate MovieScope login page

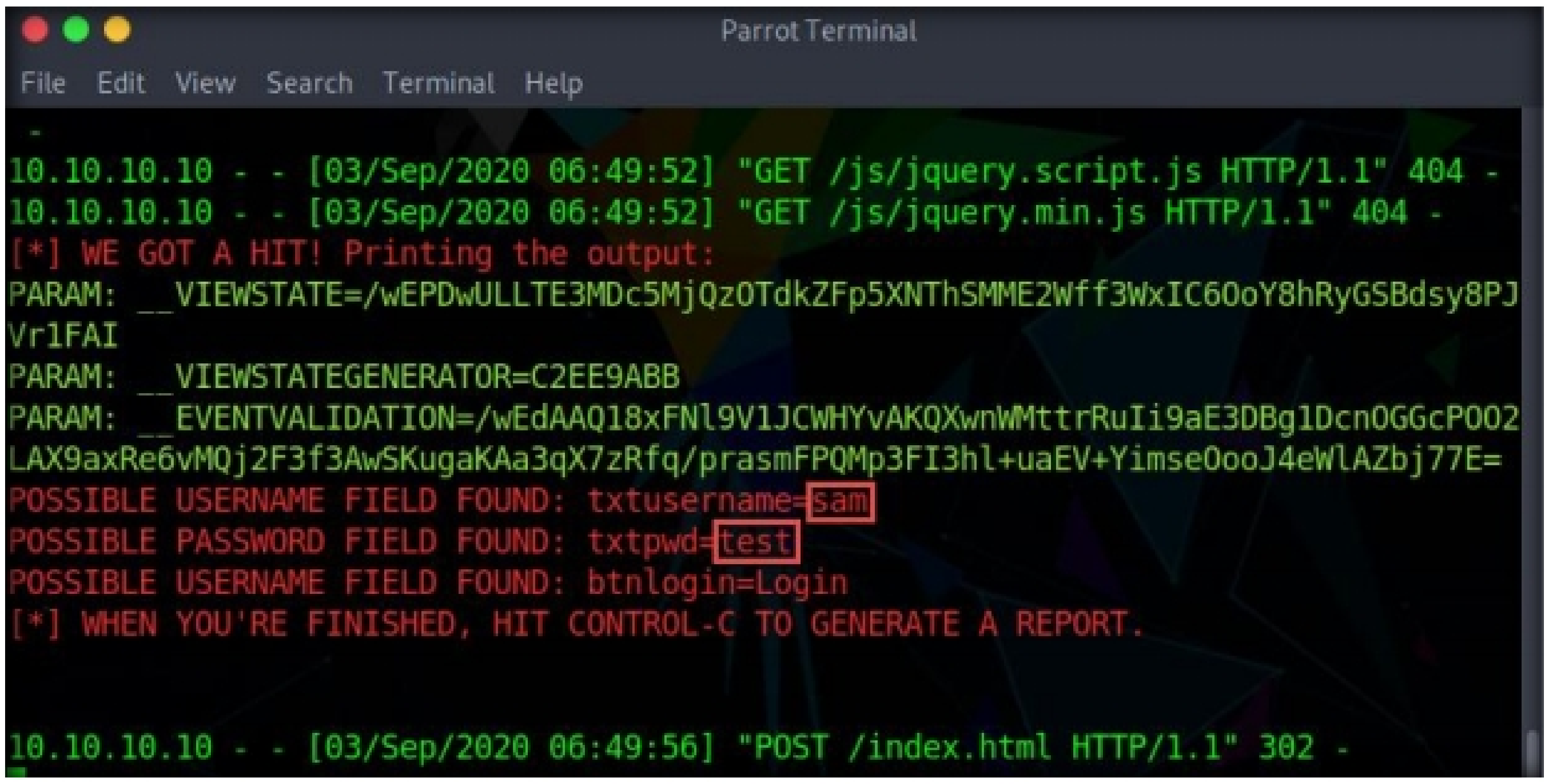
TASK 1.5

Obtain the Credentials

26. Now, switch back to the **Parrot Security** virtual machine.

27. As soon as the victim types in his/her **Username** and **Password** and clicks **Log In**, **SET** extracts the typed credentials. These can now be used by the attacker to gain unauthorized access to the victim's account.

28. Scroll down to find **Username** and **Password** displayed in plain text, as shown in the screenshot.



```
 -
10.10.10.10 - - [03/Sep/2020 06:49:52] "GET /js/jquery.script.js HTTP/1.1" 404 -
10.10.10.10 - - [03/Sep/2020 06:49:52] "GET /js/jquery.min.js HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: __VIEWSTATE=/wEPDwULLTE3MDc5MjQzOTdkZFp5XNThSMME2Wff3WxIC6OoY8hRyGSBdsy8PJ
Vr1FAI
PARAM: __VIEWSTATEGENERATOR=C2EE9ABB
PARAM: __EVENTVALIDATION=/wEdAAQ18xFNl9V1JCWHYvAKQXwnWMttrRuIi9aE3DBg1DcnOGGcPOO2
LAX9axRe6vMQj2F3f3AwSKugaKAa3qX7zRfq/prasmFPQMp3FI3hl+uaEV+YimseOooJ4eWlAZbj77E=
POSSIBLE USERNAME FIELD FOUND: txtusername=sam
POSSIBLE PASSWORD FIELD FOUND: txtpwd=test
POSSIBLE USERNAME FIELD FOUND: btnlogin=Login
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


10.10.10.10 - - [03/Sep/2020 06:49:56] "POST /index.html HTTP/1.1" 302 -
```

Figure 1.1.14: Credentials obtained by SET

Note: If you are unable to harvest the credentials then follow below steps:

- Uninstall the SEToolkit by issuing the command, **apt-get purge --auto-remove set**.
- Clone the SEToolkit repository using the command, **git clone https://github.com/trustedsec/social-engineer-toolkit**.
- Type **cd setoolkit** to navigate to the setoolkit directory.
- Navigate to the cloned repository and install the tool using command **pip3 install -r requirements.txt**.
- Issue the command, **chmod +x setoolkit** to change the file permission.
- Run the tool by issuing the command, **./setoolkit**.
- Re-perform the **Steps#3-26**.

29. This concludes the demonstration of phishing user credentials using the SET.

30. Close all open windows and document all the acquired information.

31. Turn off **Windows Server 2019** virtual machine.

TASK 2

Perform Phishing using ShellPhish

Here, we will use ShellPhish to mount a phishing attack with a cloned Instagram login page.

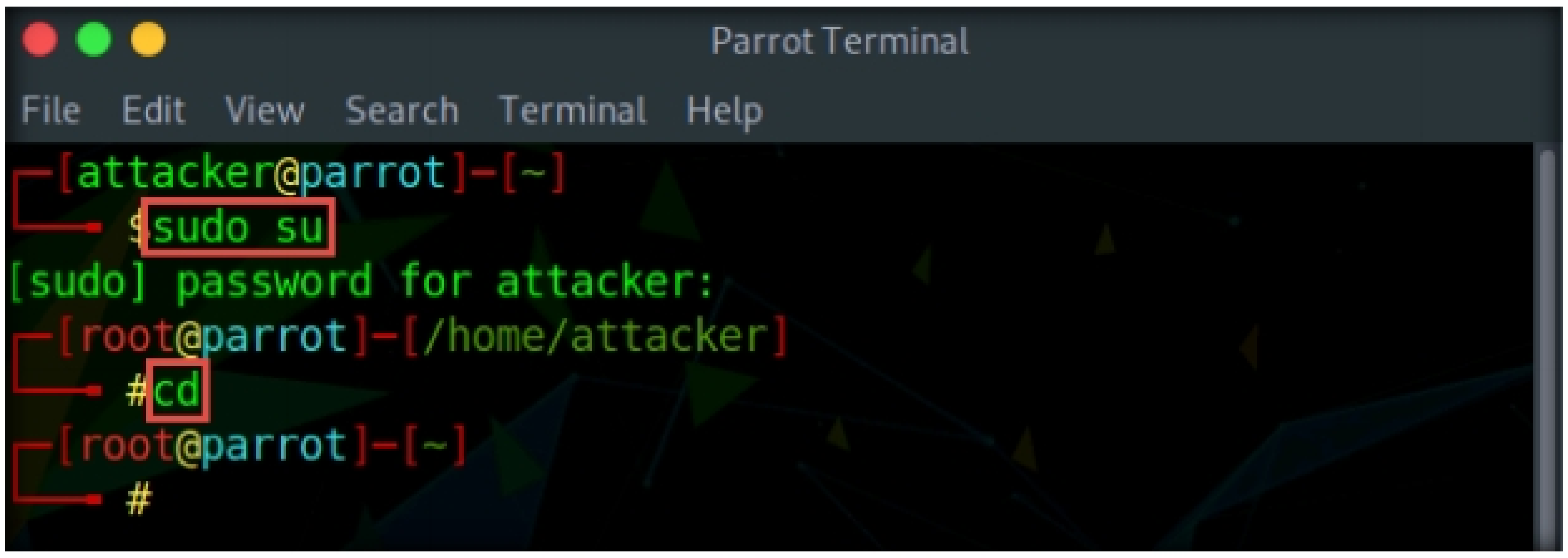
1. In the **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

In a phishing attack, an attacker poses as a legitimate website or company by registering a fake domain name, building a lookalike website, and then mailing a link to the fake website to several users. When users click on the link, they are redirected to the fake webpage, where they are lured into sharing sensitive details such as contact details, account numbers, or credit card information, without realizing that they are on a phishing site.

2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory



```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #
```

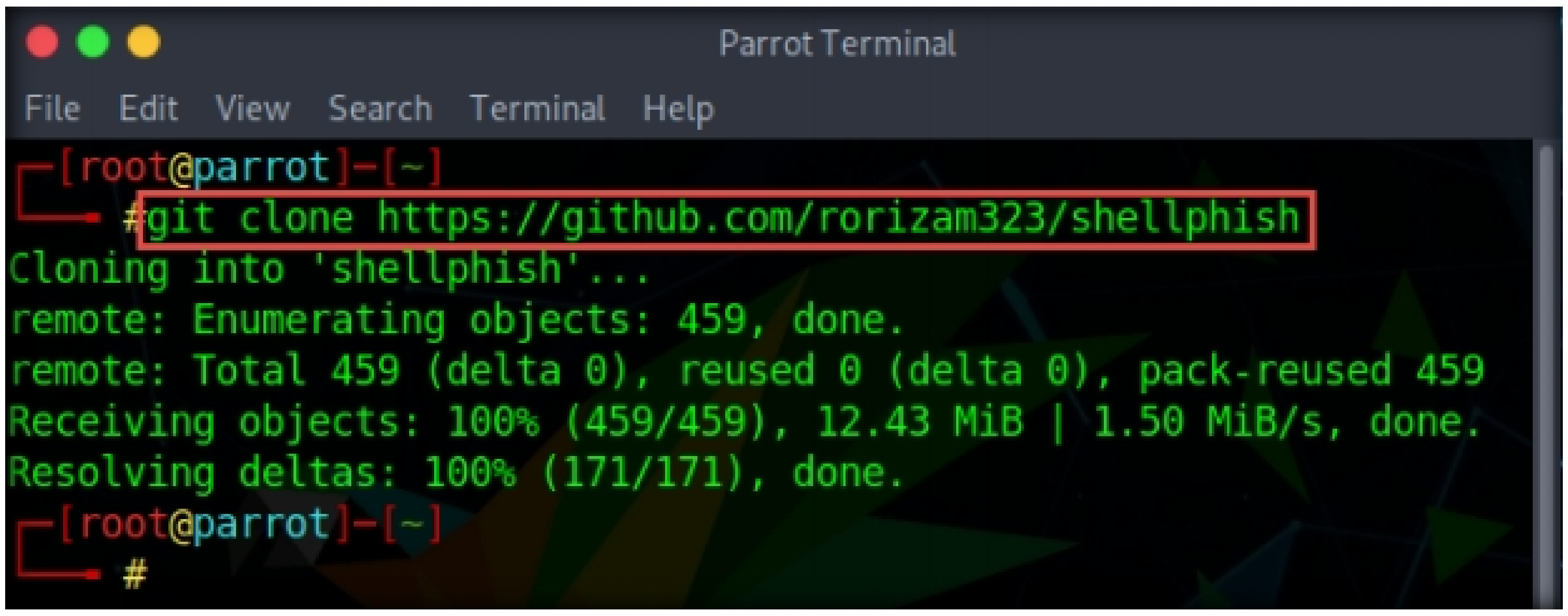
Figure 1.2.1: Running the programs as a root user

TASK 2.1

Clone ShellPhish Tool

In phishing attacks, phishers (attackers) can target individuals who avail bank and online payment services. They send messages to bank customers that claim to be from a bank and appear legitimate, because attackers use manipulated URLs and website forgery to deceive victims.

5. In the **Parrot Terminal** window, type **git clone https://github.com/rorizam323/shellphish** and press **Enter** to download the ShellPhish repository.



```
┌─[root@parrot]─[~]
└──╼ #git clone https://github.com/rorizam323/shellphish
Cloning into 'shellphish'...
remote: Enumerating objects: 459, done.
remote: Total 459 (delta 0), reused 0 (delta 0), pack-reused 459
Receiving objects: 100% (459/459), 12.43 MiB | 1.50 MiB/s, done.
Resolving deltas: 100% (171/171), done.
┌─[root@parrot]─[~]
└──╼ #
```

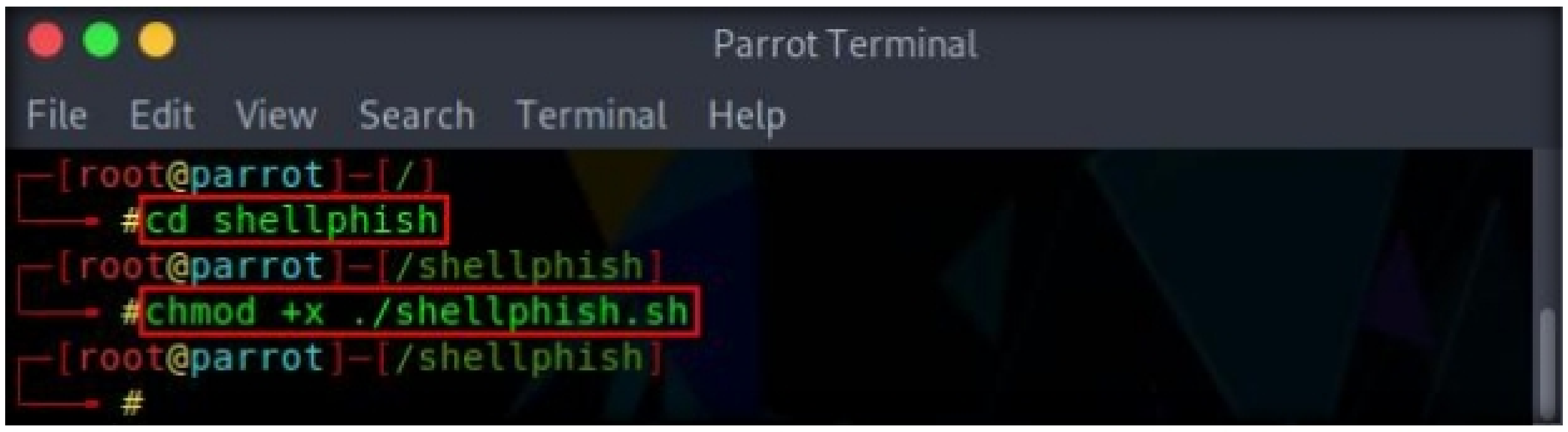
Figure 1.2.2: Cloning ShellPhish

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open any windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.

- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 09 Social Engineering/GitHub Tools/** and copy the **shellphish** folder.
- Paste the copied **shellphish** folder on the location **/home/attacker/.**
- In the terminal window, type **mv /home/attacker/shellphish /root/**.

6. Now, type **cd shellphish** and press **Enter** to navigate to the ShellPhish folder.
7. Type **chmod +x ./shellphish.sh** and press **Enter** to change the file's access permissions.



```
┌─[root@parrot]─[/]
└──╼ #cd shellphish
┌─[root@parrot]─[/shellphish]
└──╼ #chmod +x ./shellphish.sh
┌─[root@parrot]─[/shellphish]
└──╼ #
```

Figure 1.2.3: Changing the permissions of ./shellphish.sh

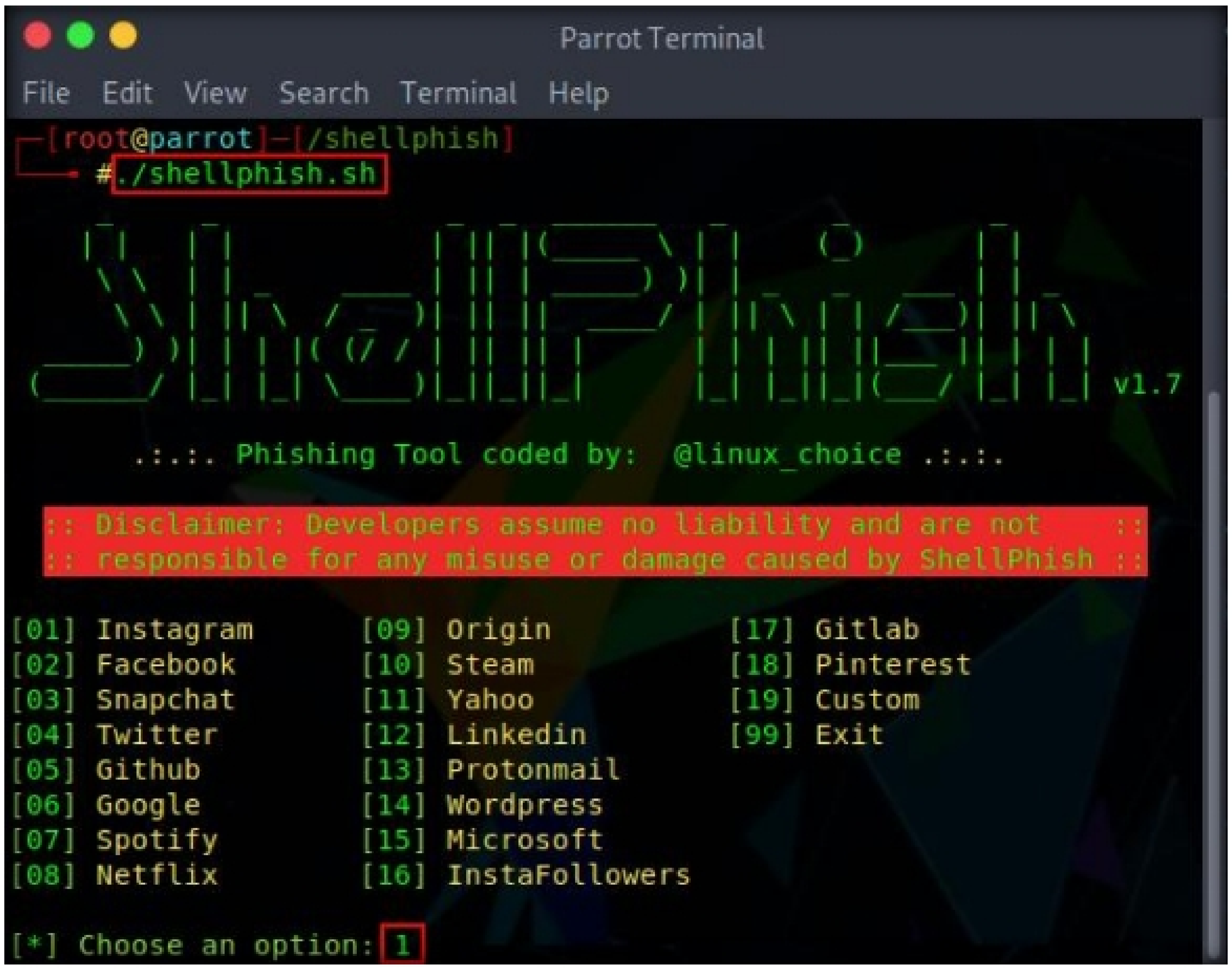
TASK 2.2

Launch ShellPhish and Generate Malicious Link

8. In the terminal window, type **./shellphish.sh** and press **Enter**.
9. The **ShellPhish** options appear; type **1** and press **Enter** to choose the **[01] Instagram** option.

Note: In this example, we will clone the Instagram login page. However, you can clone any website from the given options.

ShellPhish is a phishing tool used to obtain user credentials for various social networking platforms such as Instagram, Facebook, Twitter, and LinkedIn. It can also provide the victim system's public IP address, browser information, hostname, and geolocation.



```
┌─[root@parrot]─[/shellphish]
└──╼ #./shellphish.sh

                                                              v1.7

      .:.:. Phishing Tool coded by:  @linux_choice .:.:.

:: Disclaimer: Developers assume no liability and are not    ::
:: responsible for any misuse or damage caused by ShellPhish ::

[01] Instagram      [09] Origin          [17] Gitlab
[02] Facebook       [10] Steam           [18] Pinterest
[03] Snapchat       [11] Yahoo           [19] Custom
[04] Twitter        [12] Linkedin        [99] Exit
[05] Github         [13] Protonmail
[06] Google         [14] Wordpress
[07] Spotify        [15] Microsoft
[08] Netflix        [16] InstaFollowers

[*] Choose an option: 1
```

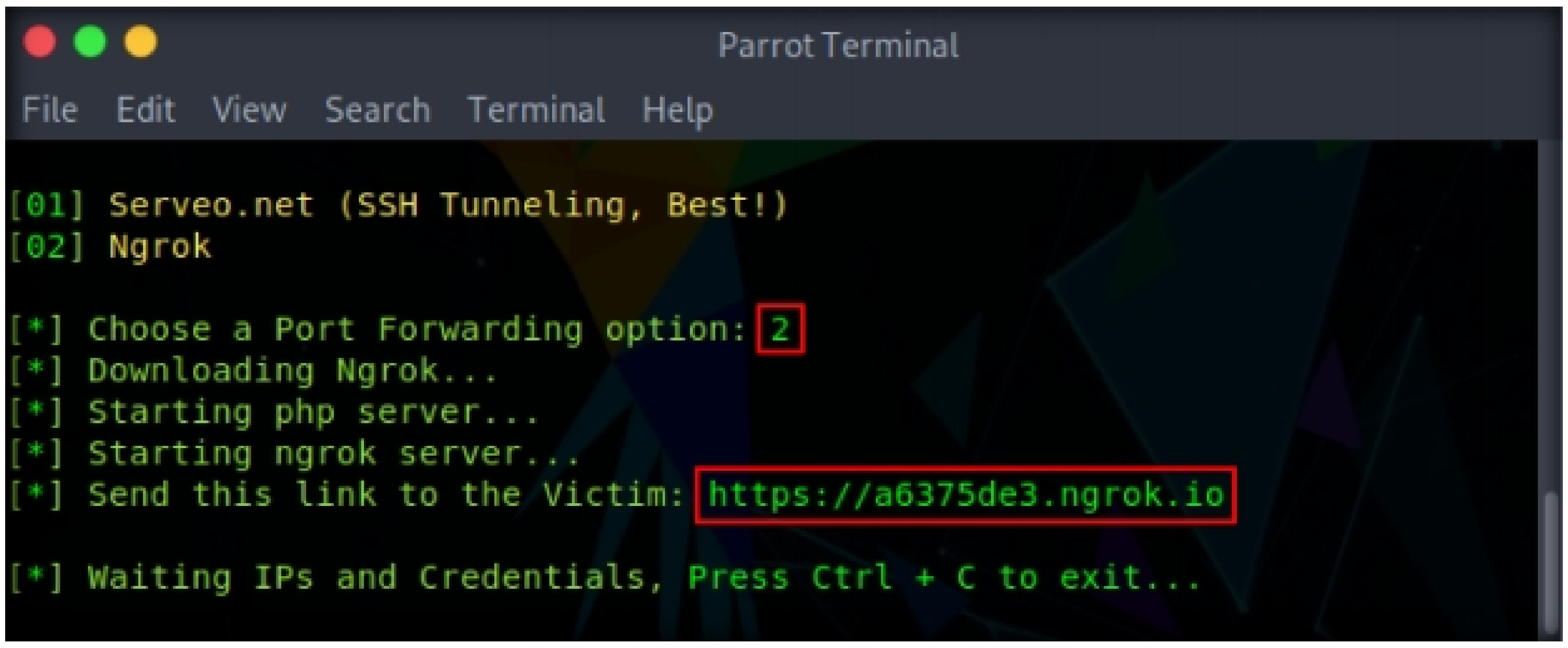
Figure 1.2.4: ShellPhish options

10. The **Choose a Port Forwarding option** appears; type **2** and press **Enter** to choose the **[02] Ngrok** option.

11. A malicious link to a cloned version of the selected social networking site appears next to the instruction **Send this link to the Victim**. Copy the link.

Not realizing that they are on a fake website, users provide their personal information and bank details. However, it is not only bank customers who are targeted, hackers are also increasingly engaging in spear-phishing campaigns against bank employees.

Note: If the malicious link is not generated, then press **Ctrl+C** to terminate the script and perform **Steps#8-10**.



```
[01] Serveo.net (SSH Tunneling, Best!)
[02] Ngrok

[*] Choose a Port Forwarding option: 2
[*] Downloading Ngrok...
[*] Starting php server...
[*] Starting ngrok server...
[*] Send this link to the Victim: https://a6375de3.ngrok.io

[*] Waiting IPs and Credentials, Press Ctrl + C to exit...
```

Figure 1.2.5: Choosing the Port Forwarding option

TASK 2.3

Create and Send a Malicious Link via Email

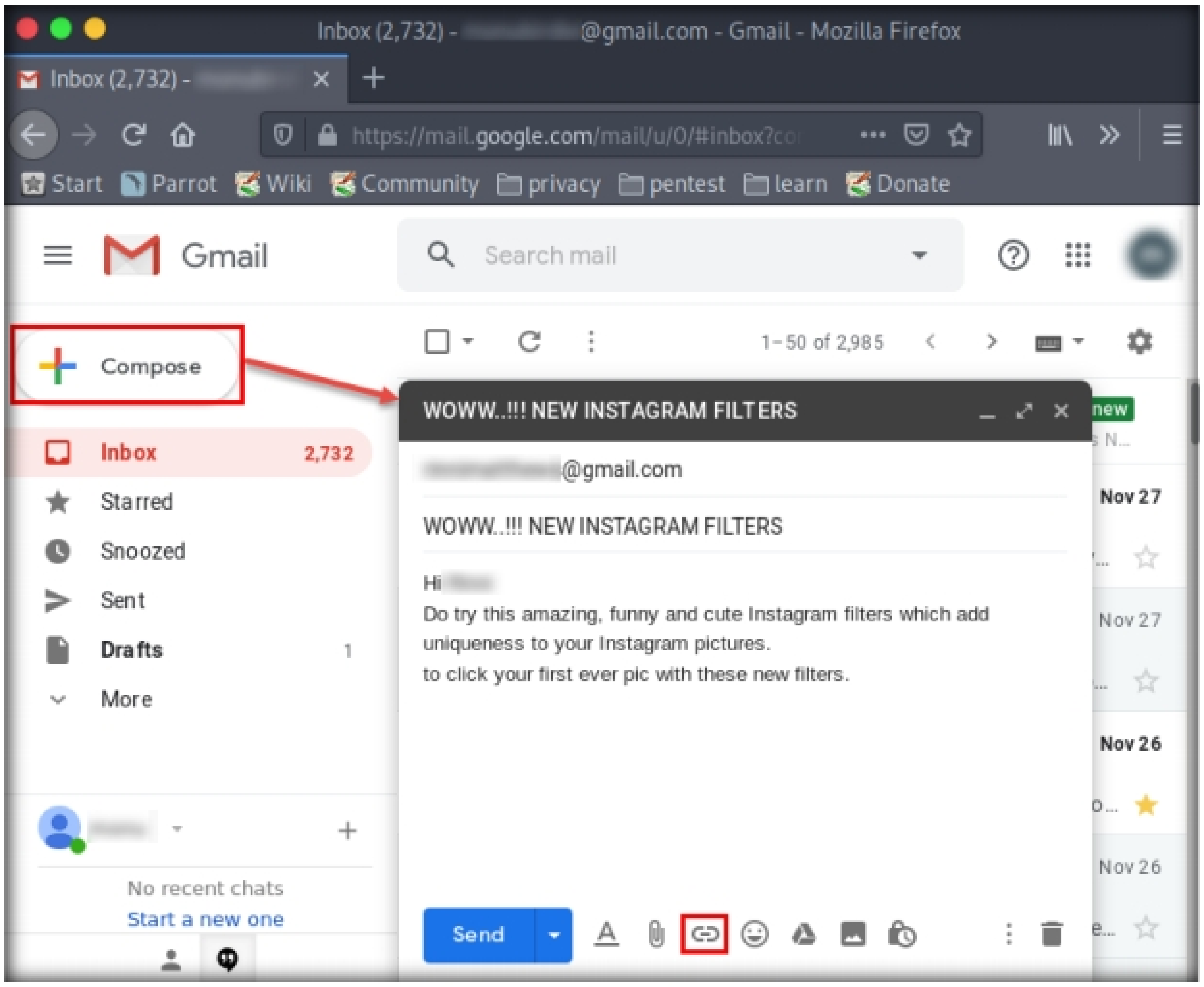
12. Having successfully created a clone website, we will now send the malicious link to the victim through an email and try to trick him/her into clicking on it.

13. Launch a web browser and open your email account (in this example, we are using **Mozilla Firefox** and **Gmail**, respectively); log in.

Note: You can use any email account of your choice.

14. After logging into your Gmail account, click the **Compose** button in the left pane and compose a fake, but enticing, email to lure a user into opening the email and clicking on a malicious link (see Task 1.3. above).

15. Position the cursor where you wish to place the fake URL in the message. Then, click the **Insert link** icon (🔗) at the bottom of the email window.


Inbox (2,732) - [redacted]@gmail.com - Gmail - Mozilla Firefox
https://mail.google.com/mail/u/0/#inbox?c
Start
Parrot
Wiki
Community
privacy
pentest
learn
Donate
Gmail
Search mail
Compose
Inbox 2,732
Starred
Snoozed
Sent
Drafts 1
More
No recent chats
Start a new one
1–50 of 2,985
Send

WOWW..!!! NEW INSTAGRAM FILTERS

[redacted]@gmail.com

WOWW..!!! NEW INSTAGRAM FILTERS

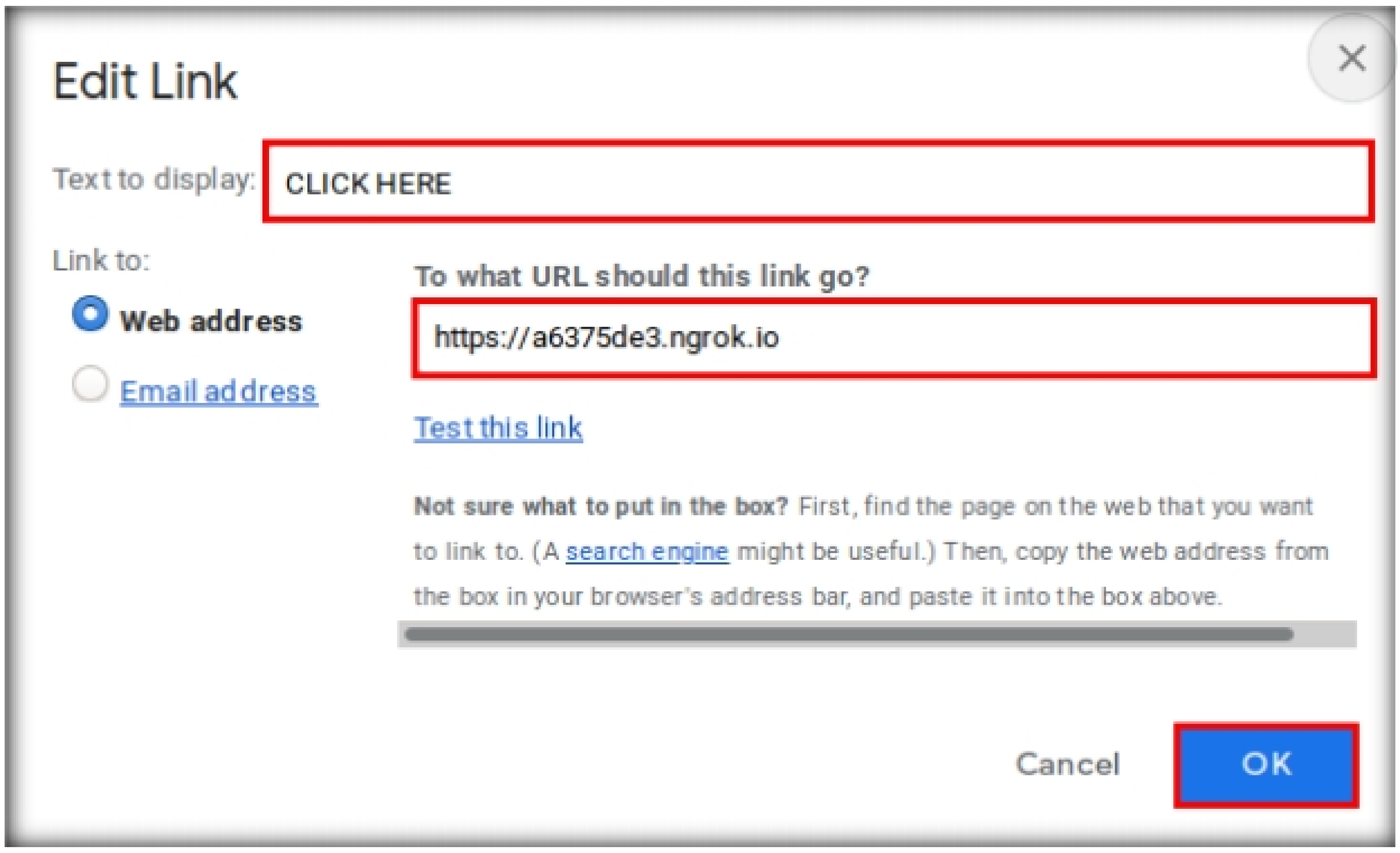
Hi [redacted]

Do try this amazing, funny and cute Instagram filters which add uniqueness to your Instagram pictures.

to click your first ever pic with these new filters.

Figure 1.2.6: Creating and concealing a malicious link

16. In the **Edit Link** window, paste the copied malicious link in the **Web address** field under the **Link to** section. In the **Text to display** field, type **CLICK HERE** and click the **OK** button.



Edit Link

Text to display: CLICK HERE

Link to:

● Web address

○ Email address

To what URL should this link go?

https://a6375de3.ngrok.io

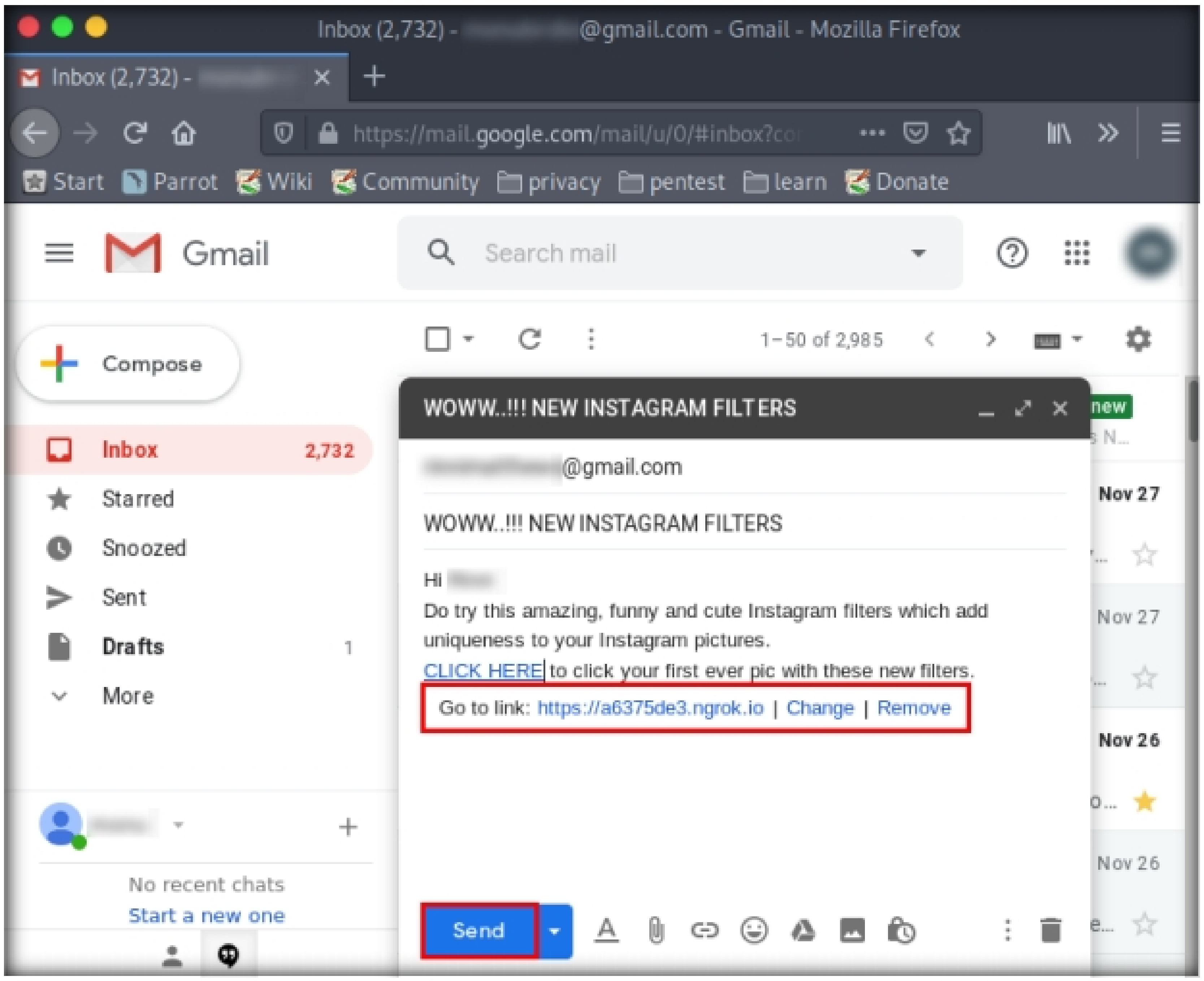
Test this link

Not sure what to put in the box? First, find the page on the web that you want to link to. (A search engine might be useful.) Then, copy the web address from the box in your browser's address bar, and paste it into the box above.

Figure 1.2.7: The Edit Link window

17. The fake link should appear in the message body, as shown in the screenshot.

18. Verify that the fake link is linked to the correct cloned site: in Gmail, click the link; the actual URL will be displayed in a "**Go to link**" pop-up. Once verified, send the email to the intended user.


Inbox (2,732) - [redacted]@gmail.com - Gmail - Mozilla Firefox
Inbox (2,732) - [redacted]
https://mail.google.com/mail/u/0/#inbox?co
Start
Parrot
Wiki
Community
privacy
pentest
learn
Donate
Gmail
Search mail
Compose
Inbox 2,732
Starred
Snoozed
Sent
Drafts 1
More
No recent chats
Start a new one
1–50 of 2,985
new
Nov 27
Nov 27
Nov 26
Nov 26
Send

WOWW..!!! NEW INSTAGRAM FILTERS

[redacted]@gmail.com

WOWW..!!! NEW INSTAGRAM FILTERS

Hi [redacted]
Do try this amazing, funny and cute Instagram filters which add uniqueness to your Instagram pictures.
CLICK HERE to click your first ever pic with these new filters.

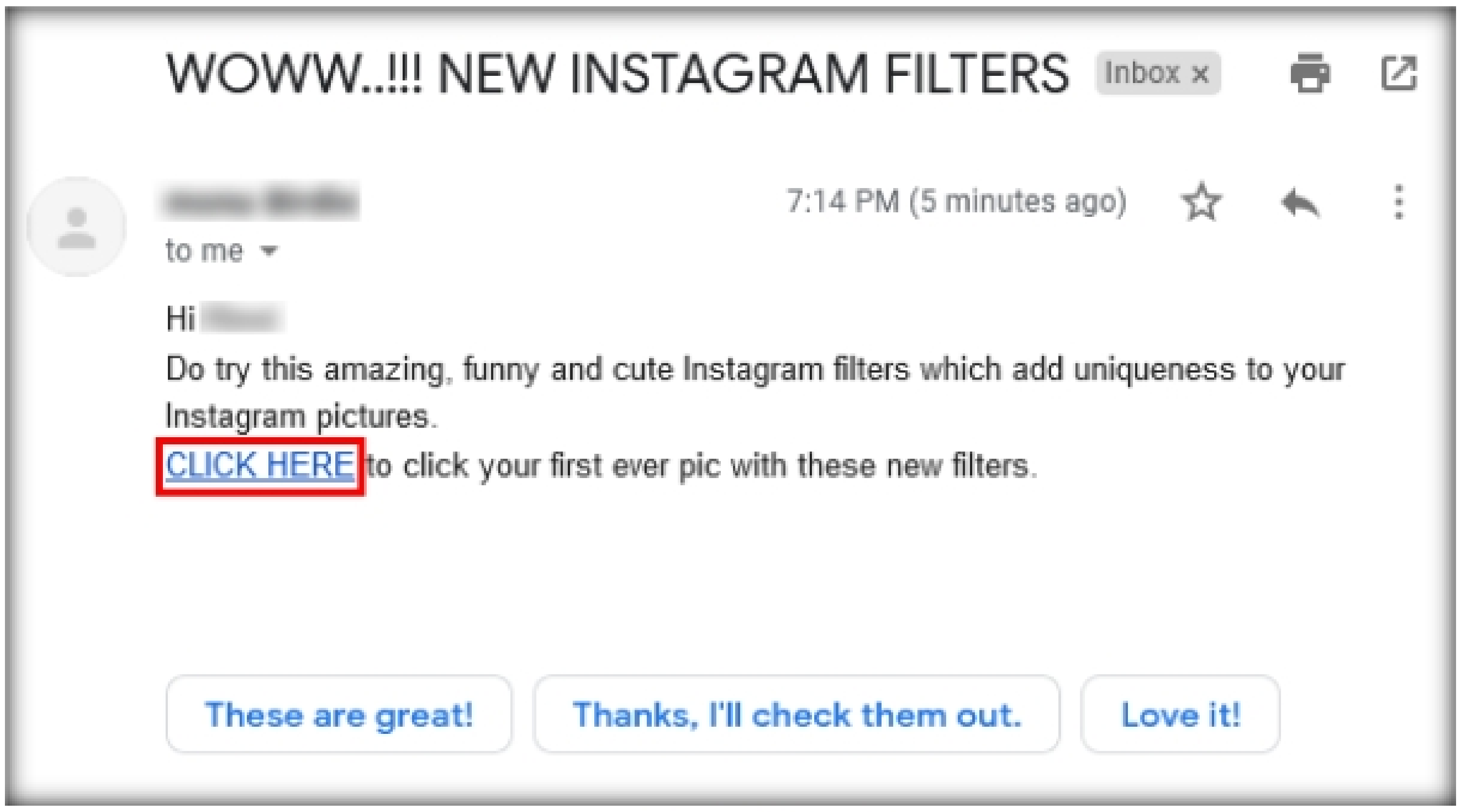
Go to link: https://a6375de3.ngrok.io | Change | Remove

Figure 1.2.8: The cloned site URL hidden in a fake link

TASK 2.4

Open Phishing Email and Log in to the Cloned Website

19. Switch to the **Windows 10** virtual machine. Open any web browser (in this example, we are using **Mozilla Firefox**), sign in to the email account to which you sent the phishing mail as an attacker. Open the email you sent previously and click **HERE** to open the malicious link.


Inbox ×
These are great!
Thanks, I'll check them out.
Love it!

WOWW..!!! NEW INSTAGRAM FILTERS

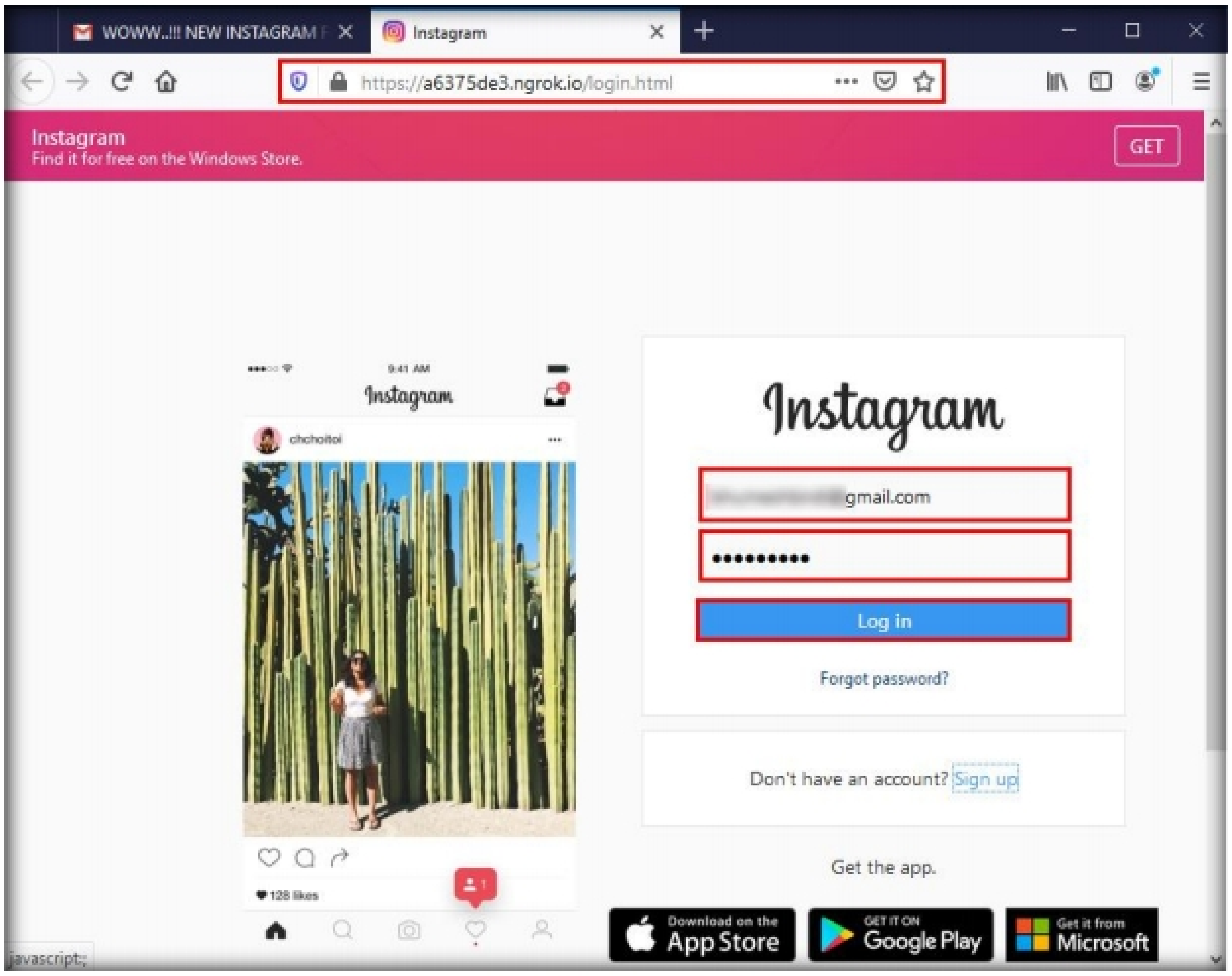
[redacted]
7:14 PM (5 minutes ago)
to me

Hi [redacted]
Do try this amazing, funny and cute Instagram filters which add uniqueness to your Instagram pictures.
CLICK HERE to click your first ever pic with these new filters.

Figure 1.2.9: Phishing email

20. When the victim (you in this case) clicks the **CLICK HERE** hyperlink, a new tab opens up, and he/she will be presented with a replica of **www.instagram.com**.

21. The victim will be prompted to enter his/her username and password into the form fields, which appears to be the genuine Instagram login page. When the victim enters the **Phone number**, **username**, or **email** and **Password** and clicks **Log In**, he/she is redirected to the legitimate **Instagram** login page. Note the different URLs in the browser address bar for the fake and real login pages.



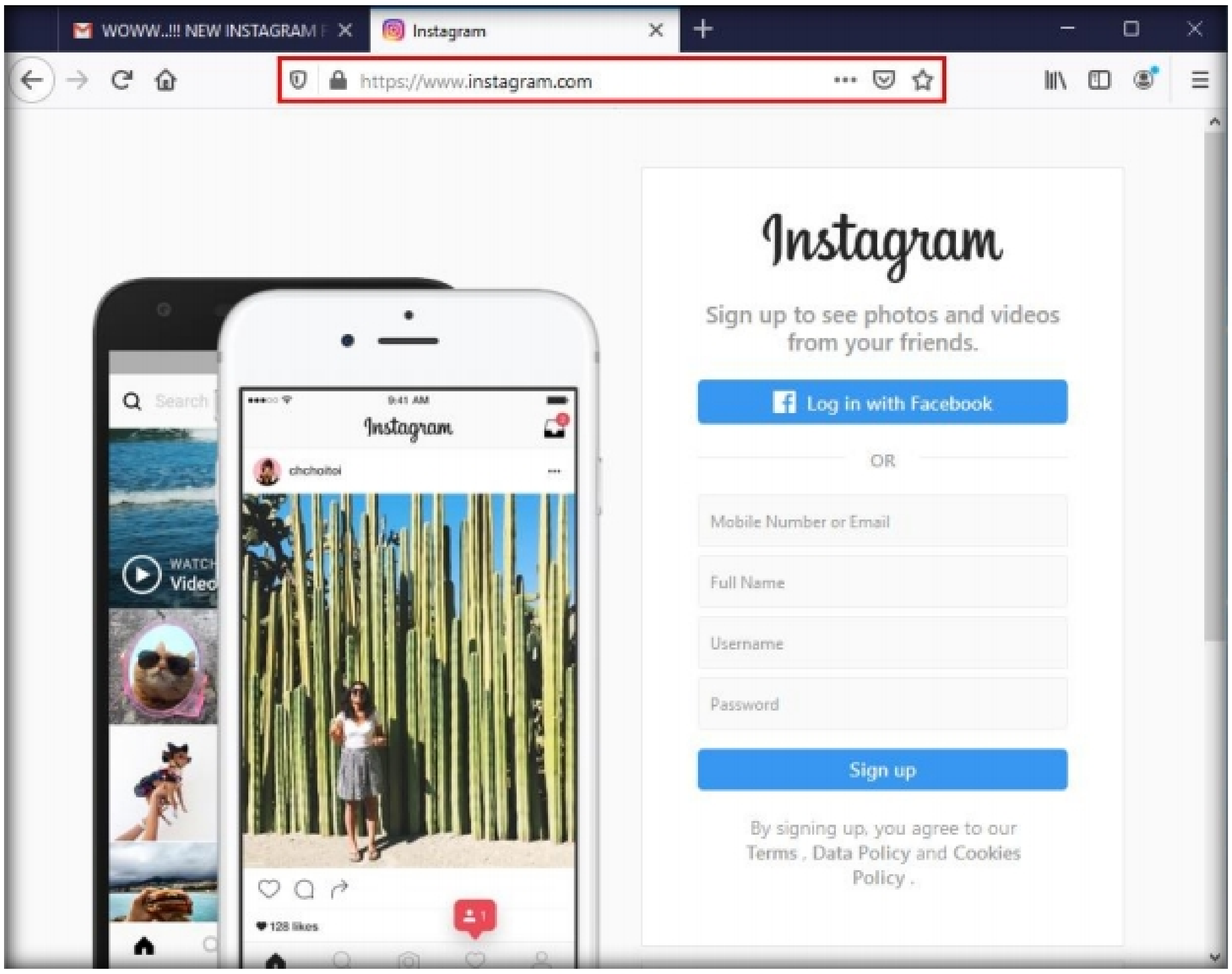
https://a6375de3.ngrok.io/login.html

[redacted]gmail.com

••••••••••

WOWW..!!! NEW INSTAGRAM F
Instagram
Instagram
Find it for free on the Windows Store.
GET
9:41 AM
Instagram
chchoitoi
128 likes
Instagram
Log in
Forgot password?
Don't have an account? Sign up
Get the app.
Download on the App Store
GET IT ON Google Play
Get it from Microsoft
javascript:;

Figure 1.2.10: Fake Instagram login page


WOWW..!!! NEW INSTAGRAM F
Instagram
https://www.instagram.com
Instagram
Log in with Facebook
OR
Mobile Number or Email
Full Name
Username
Password
Sign up
chchoitoi
128 likes
WATCH Video
Search

Sign up to see photos and videos from your friends.

By signing up, you agree to our Terms , Data Policy and Cookies Policy .

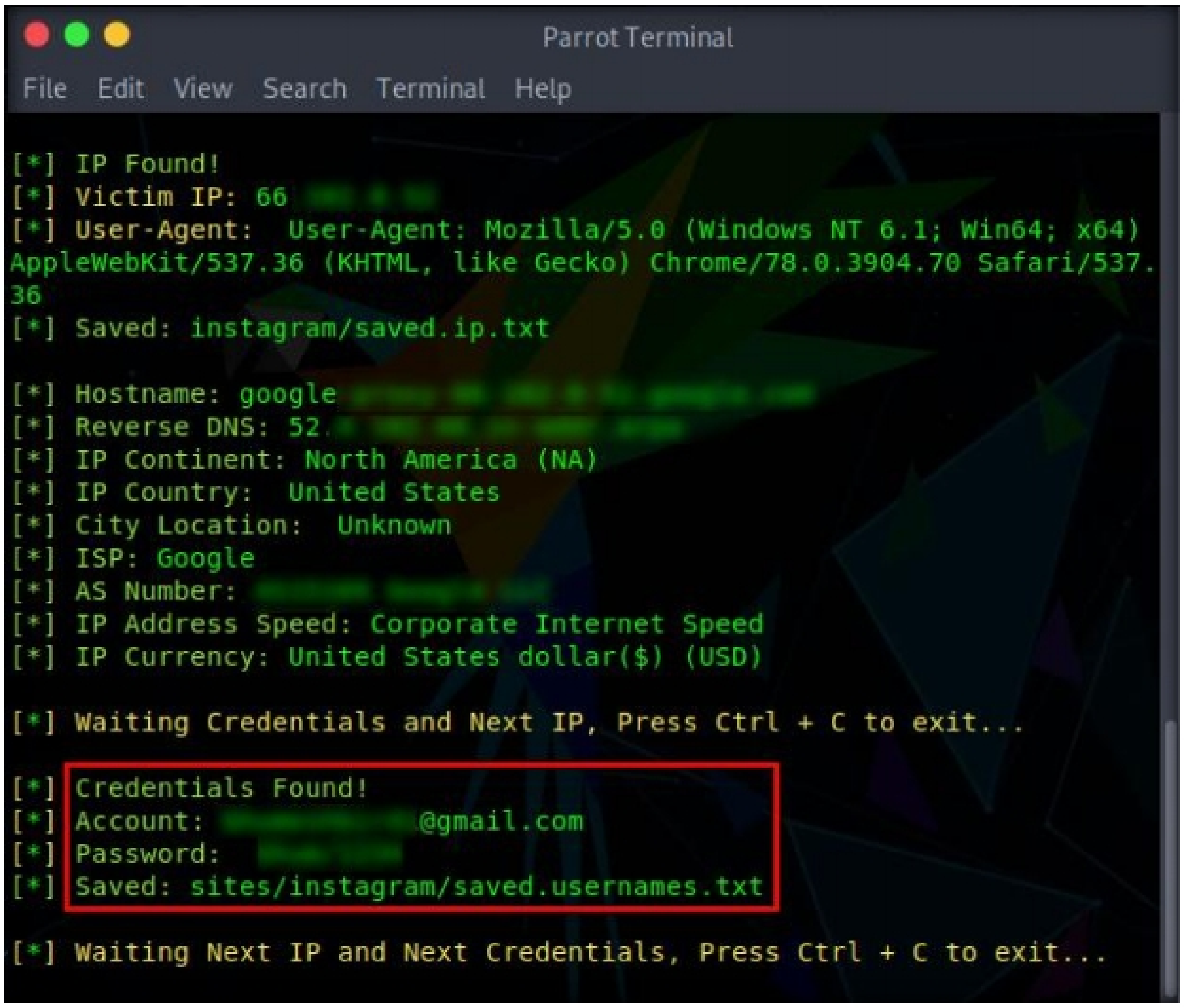
Figure 1.2.11: Legitimate Instagram login page

22. Switch back to the **Parrot Security** virtual machine and observe the terminal window running ShellPhish.

TASK 2.5

Obtain the Credentials

23. As soon as the victim opens the malicious link, information such as **Victim IP**, **User-Agent**, **Hostname**, **Reverse DNS**, and **IP Continent** is displayed, along with the obtained **Instagram** credentials. This information can be used by the attacker to gain unauthorized access to the victim's account.



```
[*] IP Found!
[*] Victim IP: 66 [redacted]
[*] User-Agent:  User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.70 Safari/537.
36
[*] Saved: instagram/saved.ip.txt

[*] Hostname: google [redacted]
[*] Reverse DNS: 52 [redacted]
[*] IP Continent: North America (NA)
[*] IP Country:  United States
[*] City Location:  Unknown
[*] ISP: Google
[*] AS Number: [redacted]
[*] IP Address Speed: Corporate Internet Speed
[*] IP Currency: United States dollar($) (USD)

[*] Waiting Credentials and Next IP, Press Ctrl + C to exit...

[*] Credentials Found!
[*] Account: [redacted]@gmail.com
[*] Password: [redacted]
[*] Saved: sites/instagram/saved.usernames.txt

[*] Waiting Next IP and Next Credentials, Press Ctrl + C to exit...
```

Figure 1.2.12: ShellPhish obtained credentials

24. This concludes the demonstration of phishing victim's credentials using ShellPhish.
25. Close all open windows and document all the acquired information.
26. Turn off the **Windows 10** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 2

Detect a Phishing Attack

Phishing is the practice of sending an illegitimate email falsely claiming to be from a legitimate site in an attempt to acquire a user's personal or account information.

ICON KEY

- 🗀 Valuable information
- ✎ Test your knowledge
- 💻 Web exercise
- 📖 Workbook review

Lab Scenario

With the tremendous increase in the use of online banking, online shares trading, and e-commerce, there has been a corresponding growth in incidents of phishing being used to carry out financial fraud.

As a professional ethical hacker or penetration tester, you must be aware of any phishing attacks that occur on the network and implement anti-phishing measures. Be warned, however, that even if you employ the most sophisticated and expensive technological solutions, these can all be bypassed and compromised if employees fall for simple social engineering scams.

The success of phishing scams is often due to users' lack of knowledge, being visually deceived, and not paying attention to security indicators. It is therefore imperative that all people in your organization are properly trained to recognize and respond to phishing attacks. It is your responsibility to educate employees about best practices for protecting systems and information. In this lab, you will learn how to detect phishing attempts using various phishing detection tools.

🗀 **Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 09 Social Engineering**

Lab Objectives

- Detect phishing using Netcraft
- Detect phishing using PhishTank

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Detecting Phishing Attempts

Phishing attacks are difficult to guard against, as the victim might not be aware that he or she has been deceived. They are very much like the other kinds of attacks used to extract a company's valuable data. To guard against phishing attacks, a company needs to evaluate the risk of different kinds of attacks, estimate possible losses and spread awareness among its employees.

Lab Tasks

TASK 1

Detect Phishing using Netcraft

Here, we will use the Netcraft Extension to detect phishing sites.

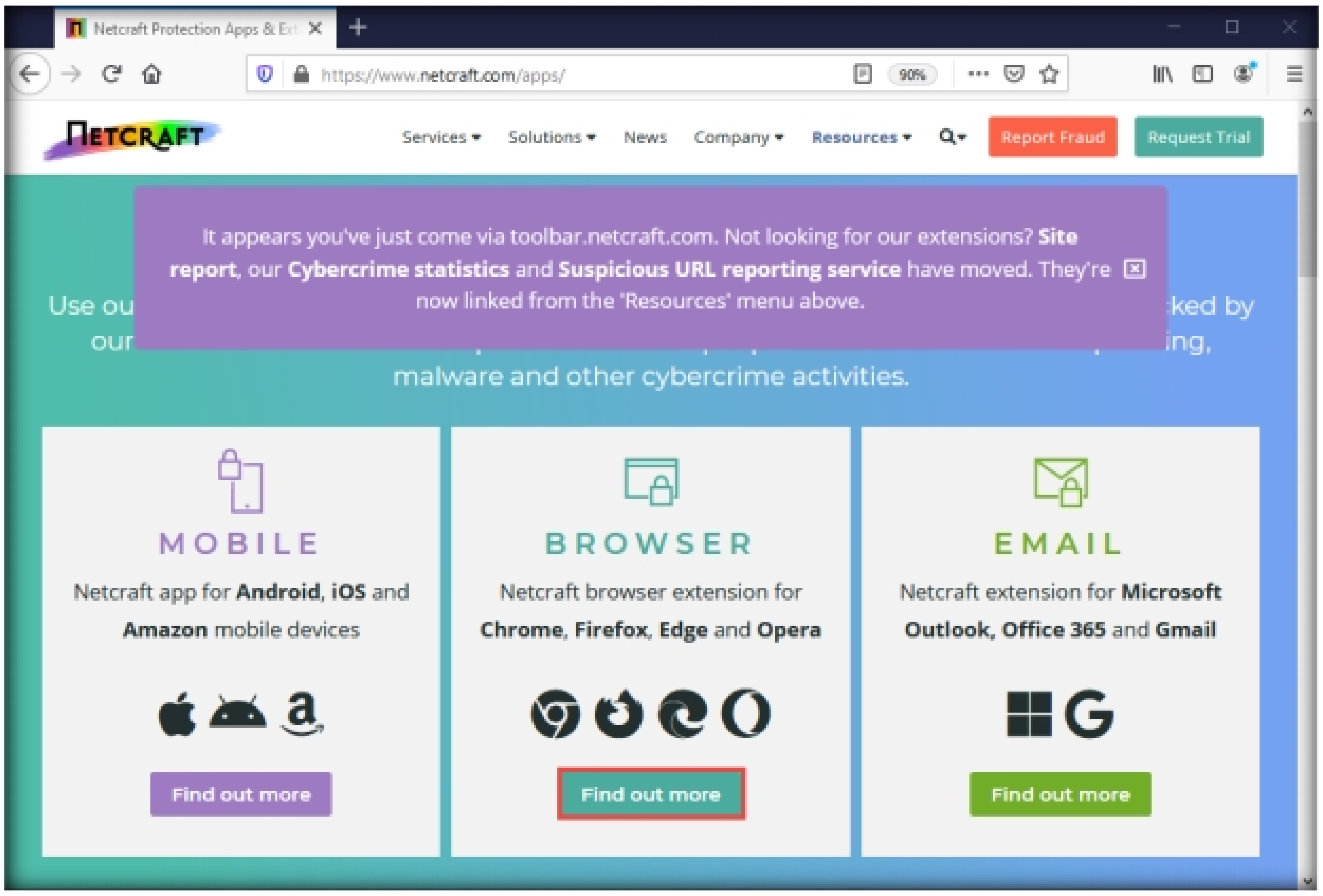
TASK 1.1

Add Netcraft Extension to the Browser

1. Turn on the **Windows 10** virtual machine and log in with the credentials **Admin**/**Pa$$w0rd**.
2. First, it is necessary to install the Netcraft extension. Open any web browser (in this example, we are using **Mozilla Firefox**), and navigate to **https://www.netcraft.com/apps/**.
3. The **Netcraft** website appears, as shown in the screenshot.
4. Click **Find out more** button under **BROWSER** option on the webpage.

The Netcraft anti-phishing community is a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks.

Note: Click **Accept** in the cookie notification in the lower section of the browse.


Netcraft Protection Apps & Ext
https://www.netcraft.com/apps/
90%
NETCRAFT
Services
Solutions
News
Company
Resources
Report Fraud
Request Trial
MOBILE
Netcraft app for Android, iOS and Amazon mobile devices
Find out more
BROWSER
Netcraft browser extension for Chrome, Firefox, Edge and Opera
Find out more
EMAIL
Netcraft extension for Microsoft Outlook, Office 365 and Gmail
Find out more

It appears you've just come via toolbar.netcraft.com. Not looking for our extensions? **Site report**, our **Cybercrime statistics** and **Suspicious URL reporting service** have moved. They're now linked from the 'Resources' menu above.

malware and other cybercrime activities.

Figure 2.1.1: The Netcraft extension page

The Netcraft Extension provides updated and extensive information about sites that users visit regularly; it also blocks dangerous sites. This information helps users to make an informed choice about the integrity of those sites.

5. In the next page, click **Download** button from the top-right corner of the webpage.

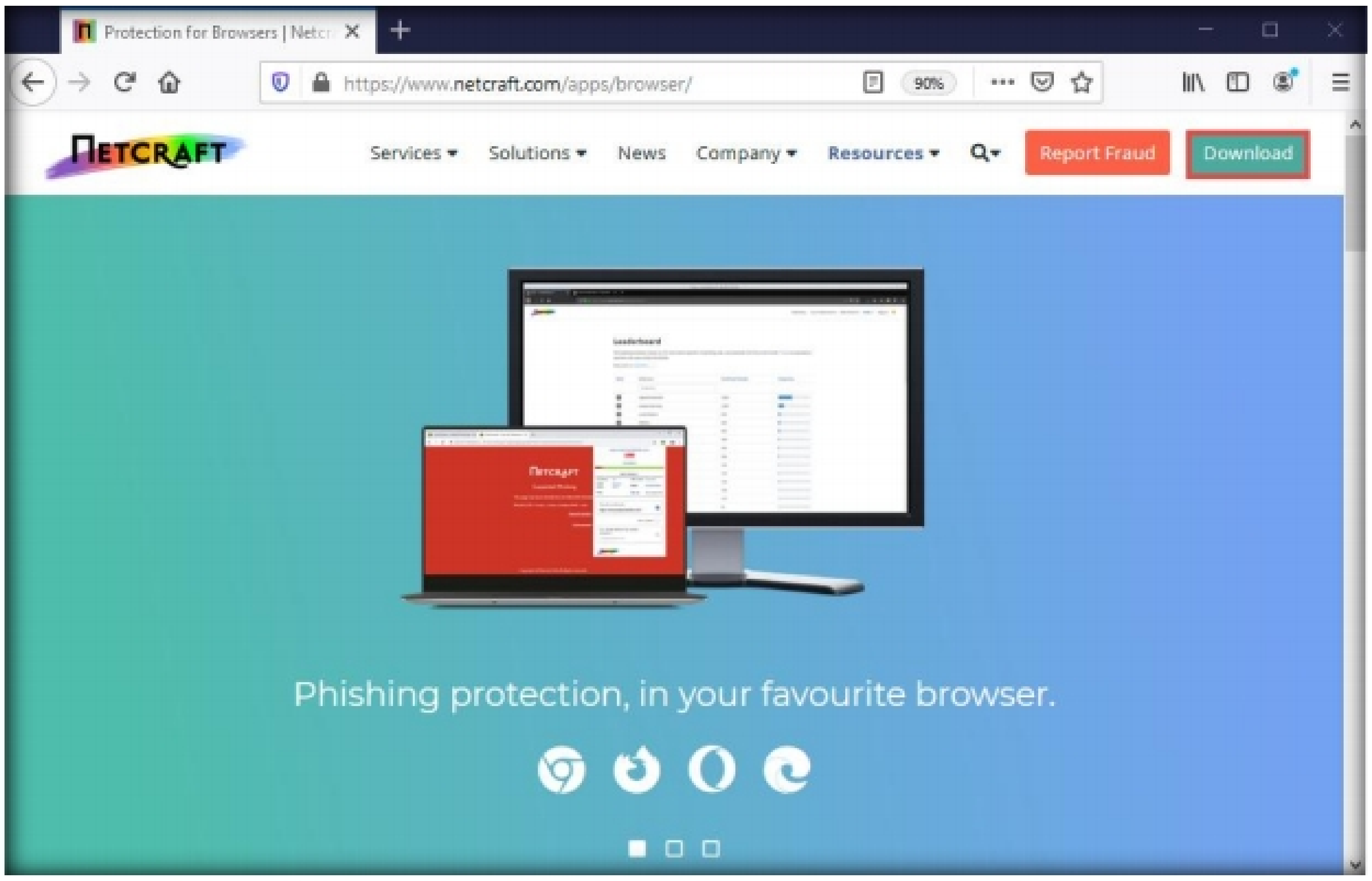

Protection for Browsers | Netcr
https://www.netcraft.com/apps/browser/
90%
NETCRAFT
Services
Solutions
News
Company
Resources
Report Fraud
Download
Phishing protection, in your favourite browser.

Figure 2.1.2: Download Netcraft

6. You will be directed to the **Get it now** section; click the **Firefox** browser icon.

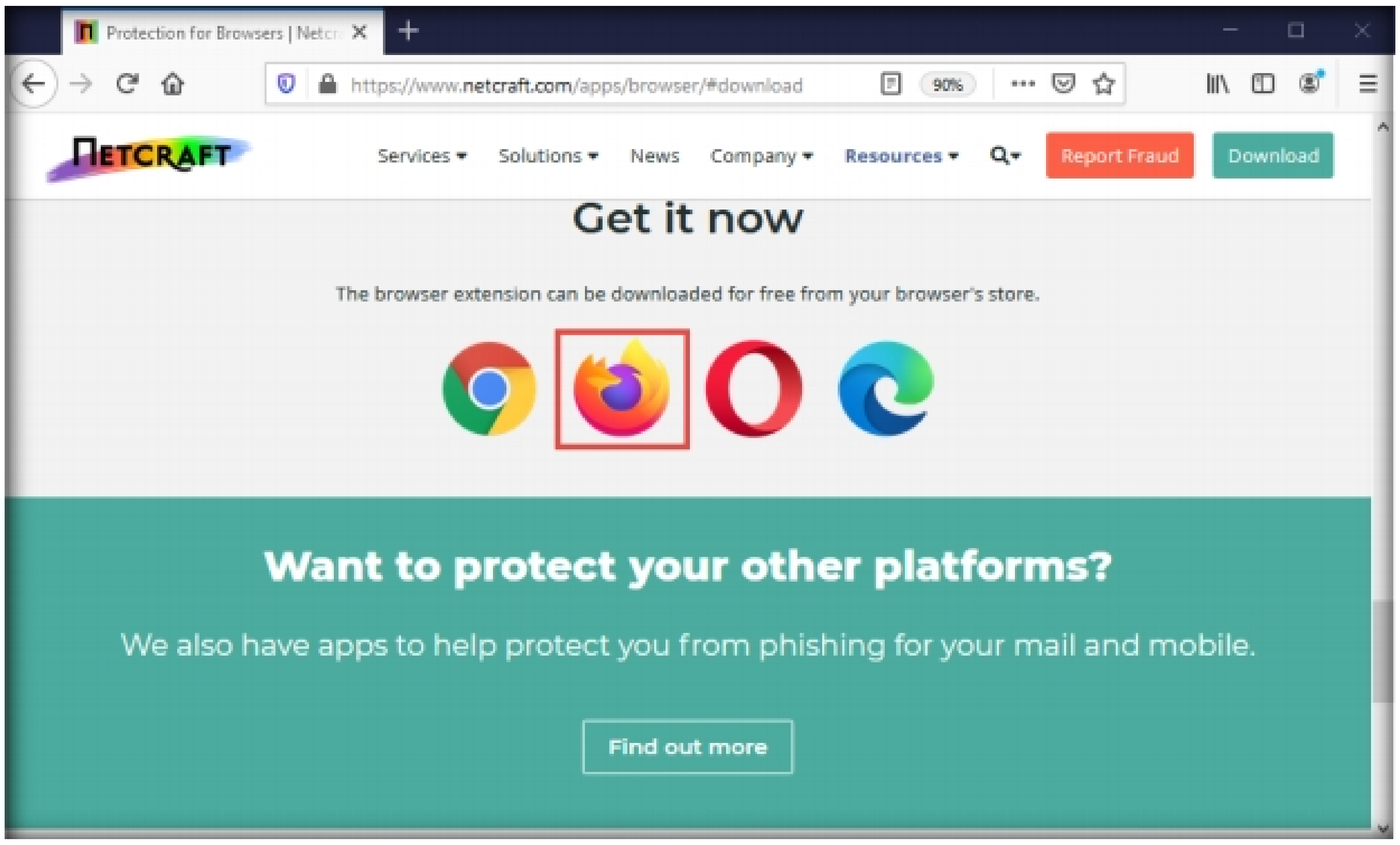
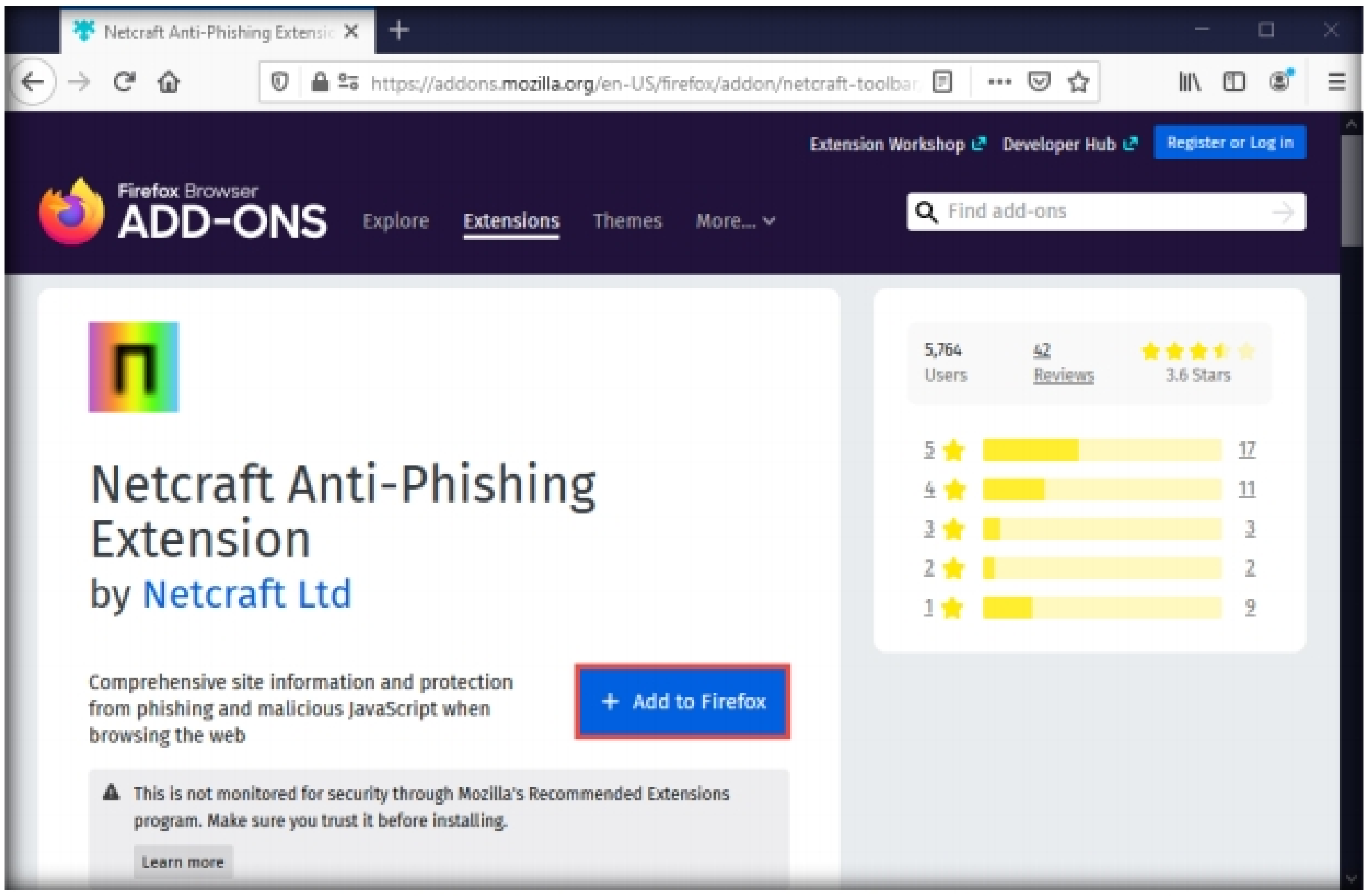

Protection for Browsers | Netcr
https://www.netcraft.com/apps/browser/#download
90%
NETCRAFT
Services
Solutions
News
Company
Resources
Report Fraud
Download
Get it now
The browser extension can be downloaded for free from your browser's store.
Want to protect your other platforms?
We also have apps to help protect you from phishing for your mail and mobile.
Find out more

Figure 2.1.3: The Netcraft extension installation page

7. On the next page, click the **Add to Firefox** button to install the Netcraft extension.


Netcraft Anti-Phishing Extensic
https://addons.mozilla.org/en-US/firefox/addon/netcraft-toolbar
Extension Workshop
Developer Hub
Register or Log in
Firefox Browser
ADD-ONS
Explore
Extensions
Themes
More...
Find add-ons
5,764
Users
42
Reviews
3.6 Stars
5
17
4
11
3
3
2
2
1
9
+ Add to Firefox
Learn more

Netcraft Anti-Phishing Extension
by Netcraft Ltd

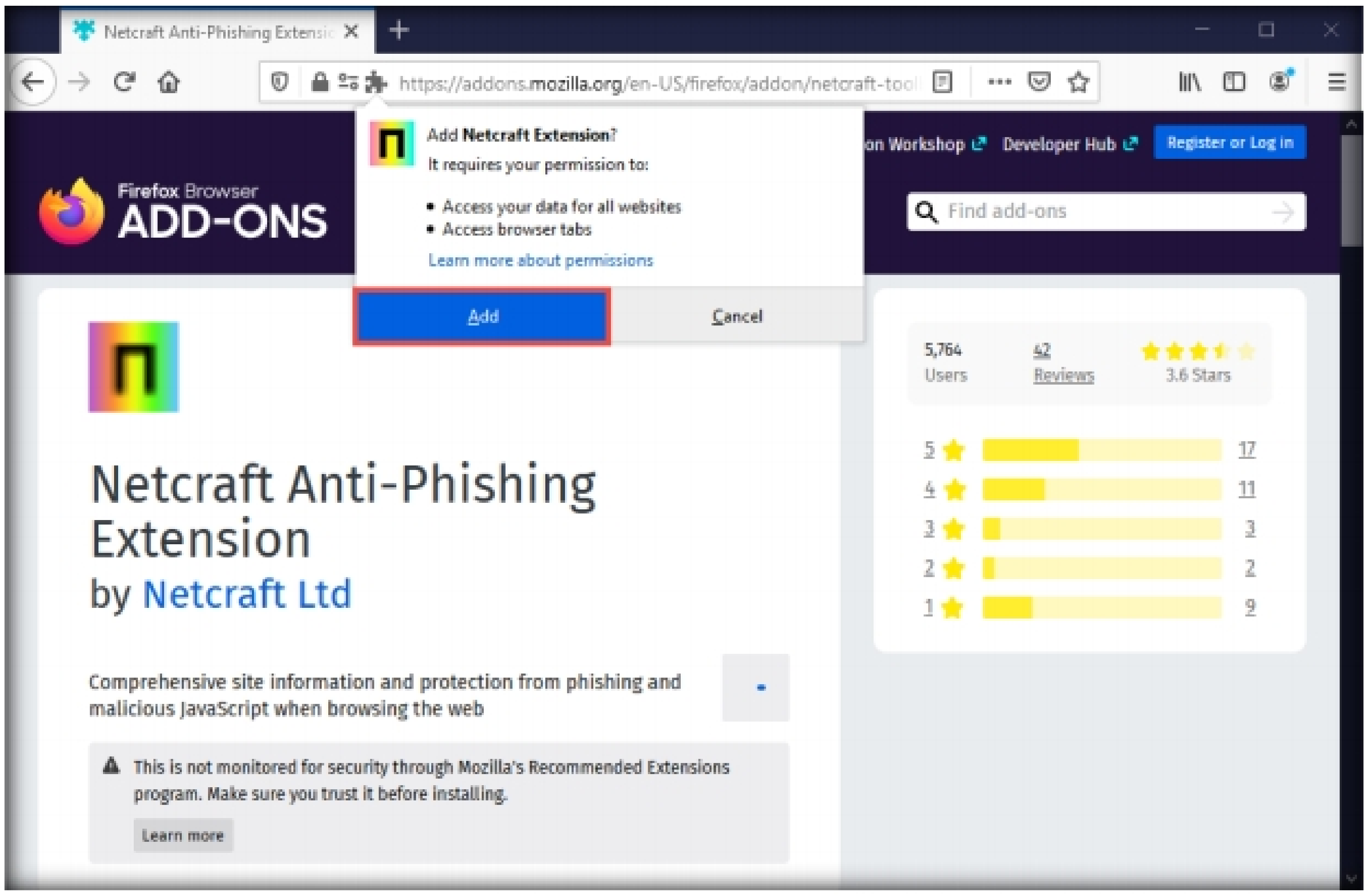
Comprehensive site information and protection from phishing and malicious JavaScript when browsing the web

This is not monitored for security through Mozilla's Recommended Extensions program. Make sure you trust it before installing.

Figure 2.1.4: Netcraft extension installation: Add to Firefox

8. When the **Add Netcraft Extension?** notification pop-up appears on top of the window, click **Add**.

Note: If the **Netcraft Extension has been added to Firefox** pop-up appears in the top section of the browser, click **Okay, Got It**.


Netcraft Anti-Phishing Extensic
https://addons.mozilla.org/en-US/firefox/addon/netcraft-tool
on Workshop
Developer Hub
Register or Log in
Firefox Browser
ADD-ONS
Find add-ons
Add
Cancel
5,764
Users
42
Reviews
3.6 Stars
5
17
4
11
3
3
2
2
1
9
Learn more

Add **Netcraft Extension**?
It requires your permission to:
- Access your data for all websites
- Access browser tabs

Learn more about permissions

Netcraft Anti-Phishing Extension
by Netcraft Ltd

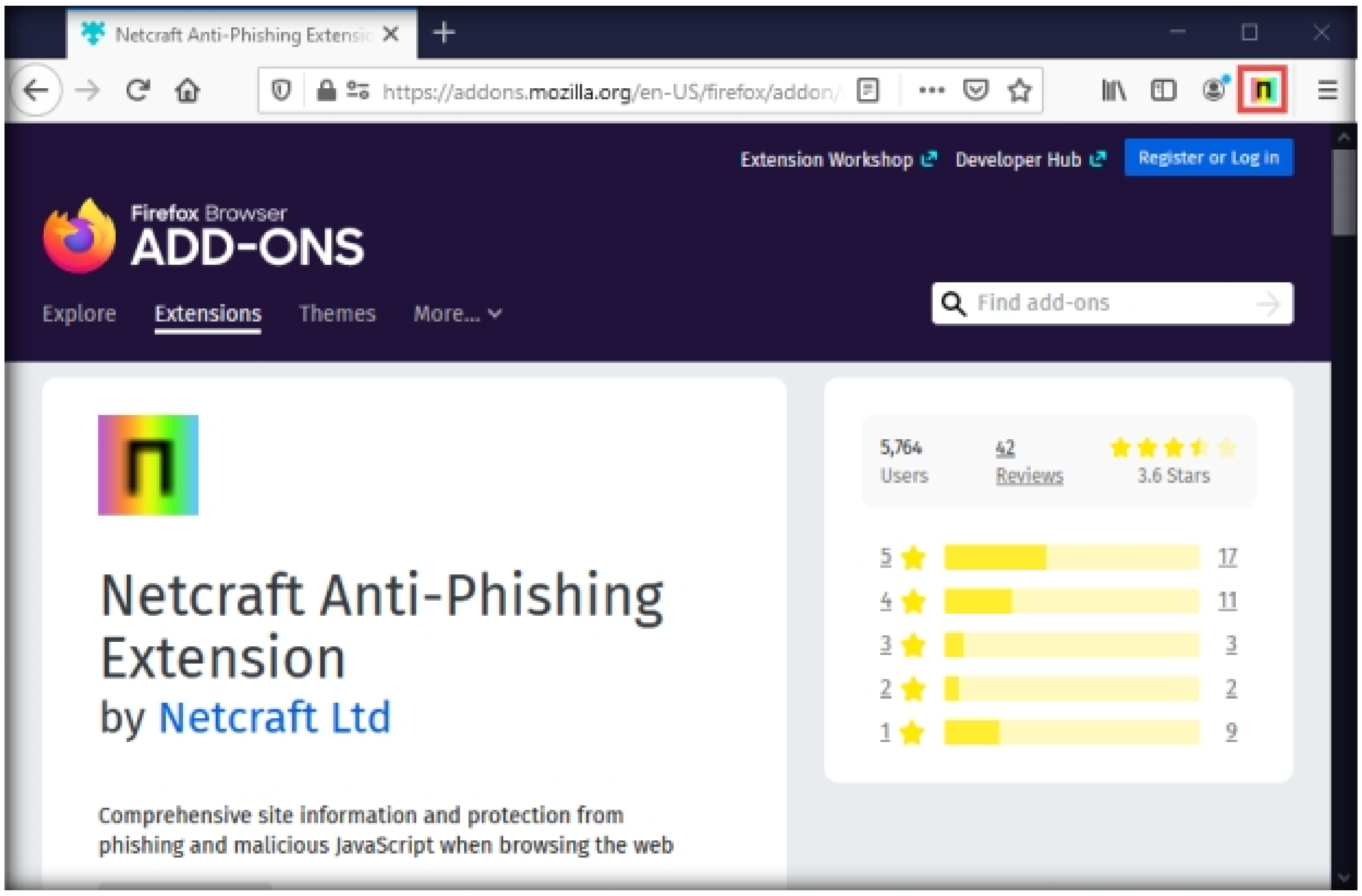
Comprehensive site information and protection from phishing and malicious JavaScript when browsing the web

This is not monitored for security through Mozilla's Recommended Extensions program. Make sure you trust it before installing.

Figure 2.1.5: Installing the Netcraft extension

9. After the installation finishes, you may be asked to restart the browser. If so, click **Restart Now**.
10. The **Netcraft Extension has been added to Firefox** notification appears, click **Okay, Got it**.
11. The **Netcraft Extension** icon now appears on the top-right corner of the browser, as shown in the screenshot.

Note: Screenshots may differ with newer versions of Firefox.


Netcraft Anti-Phishing Extensio
https://addons.mozilla.org/en-US/firefox/addon/
Extension Workshop
Developer Hub
Register or Log in
Firefox Browser
ADD-ONS
Explore
Extensions
Themes
More...
Find add-ons
Netcraft Anti-Phishing Extension
by Netcraft Ltd
5,764 Users
42 Reviews
3.6 Stars
5 17
4 11
3 3
2 2
1 9

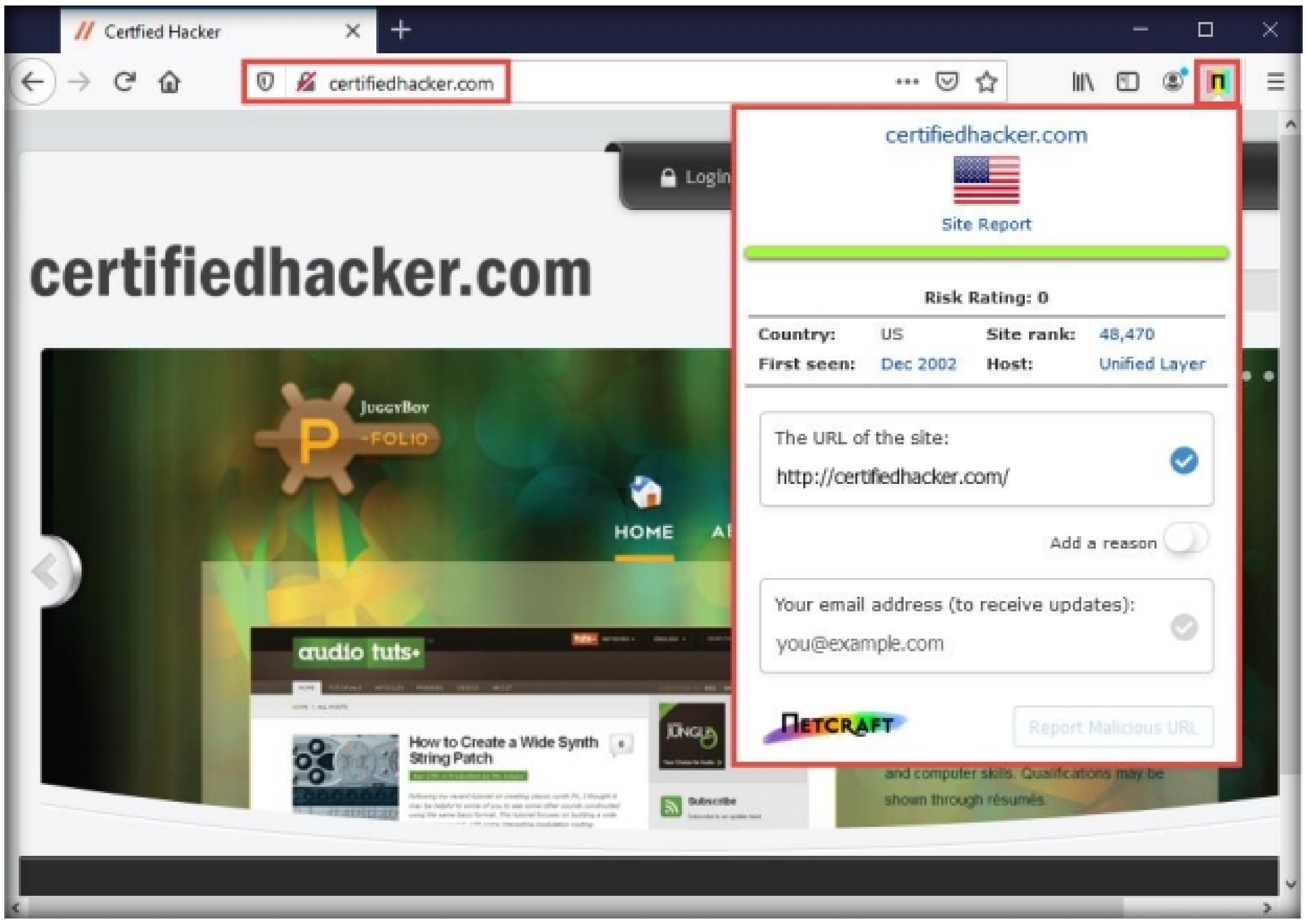
Comprehensive site information and protection from phishing and malicious JavaScript when browsing the web

Figure 2.1.6: The Netcraft extension icon

TASK 1.2

Examine Websites

12. Now, in the address bar, type **http://certifiedhacker.com/** and press **Enter**.
13. The **certifiedhacker.com** webpage appears. Click the **Netcraft Extension** icon ( ) in the top-right corner of the browser. A dialog box appears, displaying a summary of information such as **Risk Rating**, **Site rank**, **First seen**, and **Host** about the searched website.


Certfied Hacker
certifiedhacker.com
Login
HOME
audio tuts+
How to Create a Wide Synth String Patch
NETCRAFT
Report Malicious URL

certifiedhacker.com

Site Report

Risk Rating: 0

Country: US Site rank: 48,470

First seen: Dec 2002 Host: Unified Layer

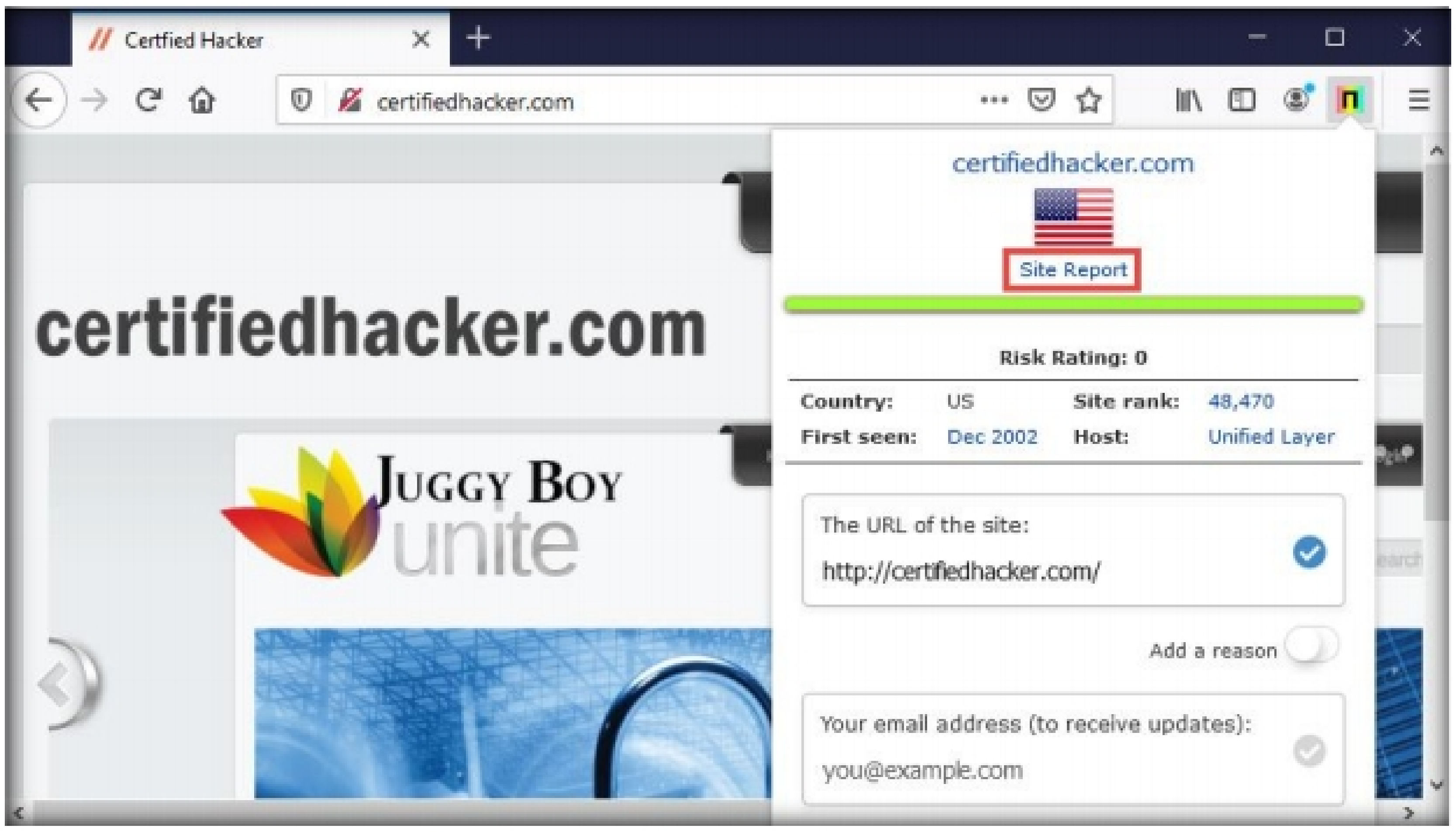
The URL of the site: http://certifiedhacker.com/

Add a reason

Your email address (to receive updates): you@example.com

Figure 2.1.7: The Netcraft extension on Mozilla Firefox

14. Now, click the **Site Report** link from the dialog-box to view a report of the site.


Certfied Hacker
certifiedhacker.com
JUGGY BOY unite

certifiedhacker.com

Site Report

Risk Rating: 0

Country: US Site rank: 48,470

First seen: Dec 2002 Host: Unified Layer

The URL of the site: http://certifiedhacker.com/

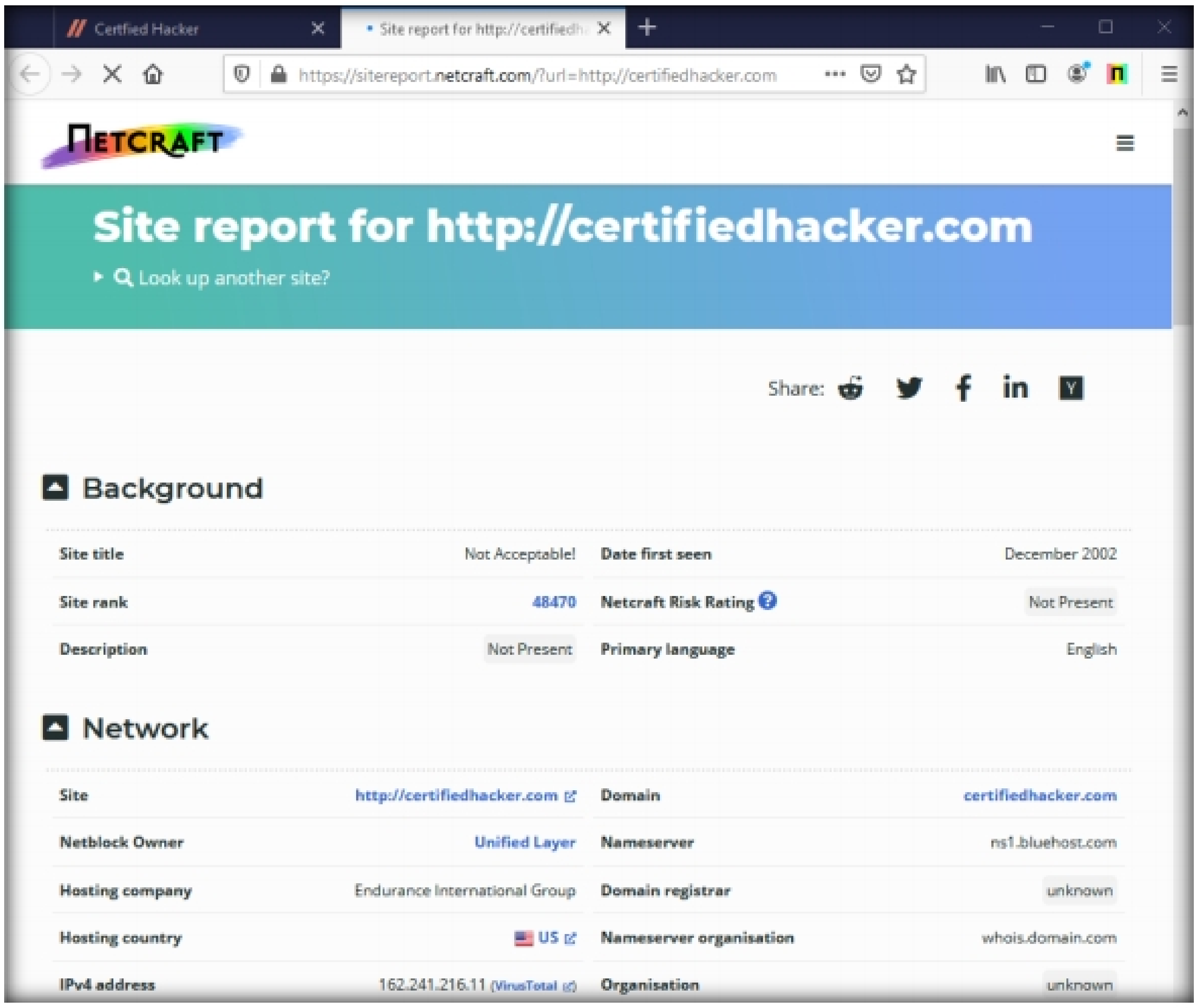
Add a reason

Your email address (to receive updates): you@example.com

Figure 2.1.8: Click Site Report

15. The **Site report for certifiedhacker.com** page appears, displaying detailed information about the site such as **Background**, **Network**, **IP delegation**, **SSL/TLS**, **Hosting History**, etc.

Note: If a **Site information not available** pop-up appears, ignore it.


Certfied Hacker
Site report for http://certifiedh
https://sitereport.netcraft.com/?url=http://certifiedhacker.com
NETCRAFT
Share:

Site report for http://certifiedhacker.com

Look up another site?

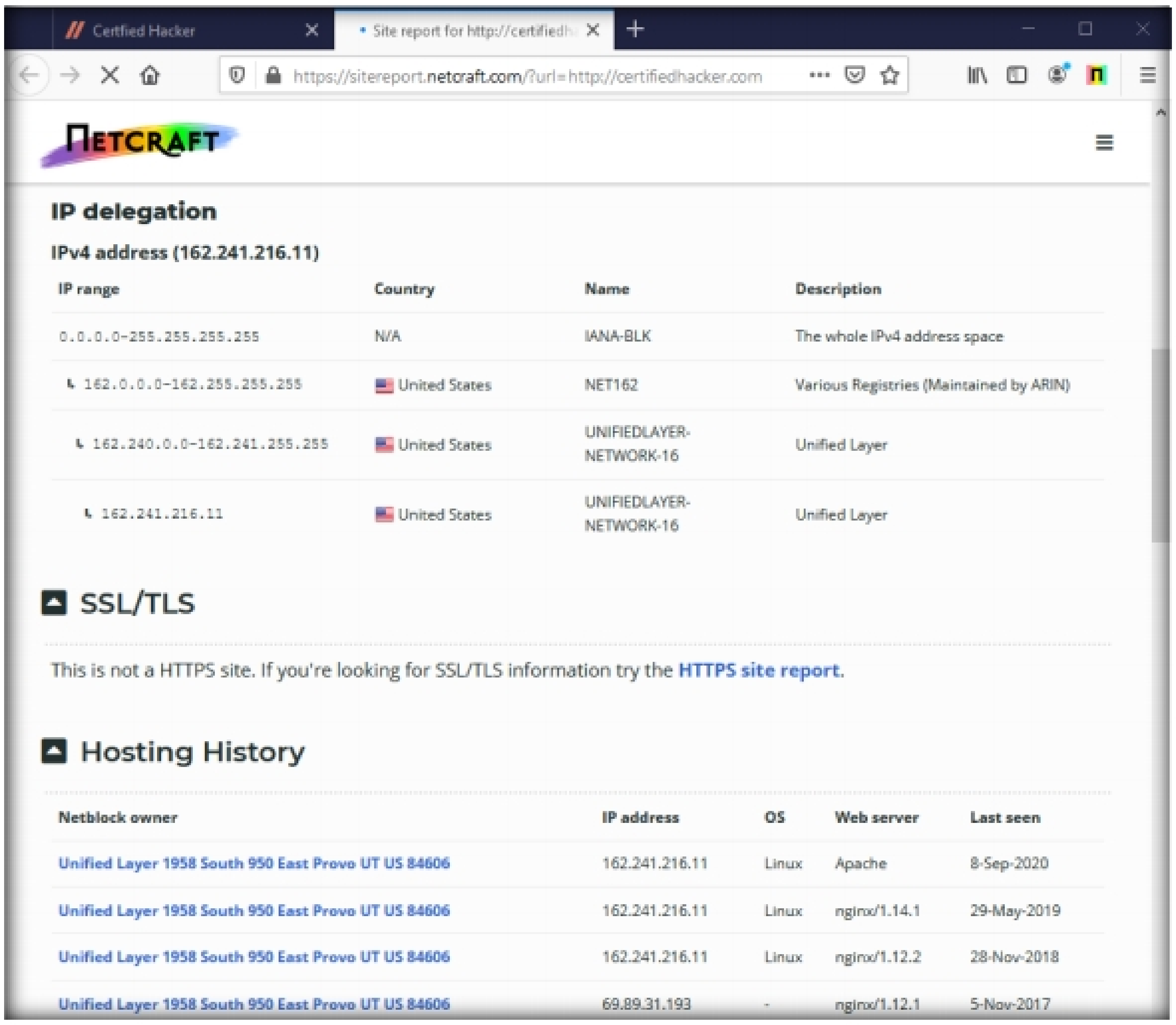
Background

Site title	Not Acceptable!	Date first seen	December 2002
Site rank	48470	Netcraft Risk Rating	Not Present
Description	Not Present	Primary language	English

Network

Site	http://certifiedhacker.com	Domain	certifiedhacker.com
Netblock Owner	Unified Layer	Nameserver	ns1.bluehost.com
Hosting company	Endurance International Group	Domain registrar	unknown
Hosting country	US	Nameserver organisation	whois.domain.com
IPv4 address	162.241.216.11 (VirusTotal)	Organisation	unknown

Figure 2.1.9: Site report generated by the Netcraft extension showing Background and Network information


Certfied Hacker
Site report for http://certifiedh
https://sitereport.netcraft.com/?url=http://certifiedhacker.com
NETCRAFT

IP delegation

IPv4 address (162.241.216.11)

IP range	Country	Name	Description
0.0.0.0-255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
↳ 162.0.0.0-162.255.255.255	United States	NET162	Various Registries (Maintained by ARIN)
↳ 162.240.0.0-162.241.255.255	United States	UNIFIEDLAYER-NETWORK-16	Unified Layer
↳ 162.241.216.11	United States	UNIFIEDLAYER-NETWORK-16	Unified Layer

SSL/TLS

This is not a HTTPS site. If you're looking for SSL/TLS information try the HTTPS site report.

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	Apache	8-Sep-2020
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	nginx/1.14.1	29-May-2019
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	nginx/1.12.2	28-Nov-2018
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	-	nginx/1.12.1	5-Nov-2017

Figure 2.1.10: Site report generated by the Netcraft extension showing IP delegation, SSL/TLS and Hosting History

TASK 1.3

Identify Phishing Site

16. If you attempt to visit a website that has been identified as a phishing site by the **Netcraft Extension**, you will see a pop-up alerting you to **Suspected Phishing**, as shown in the screenshot.

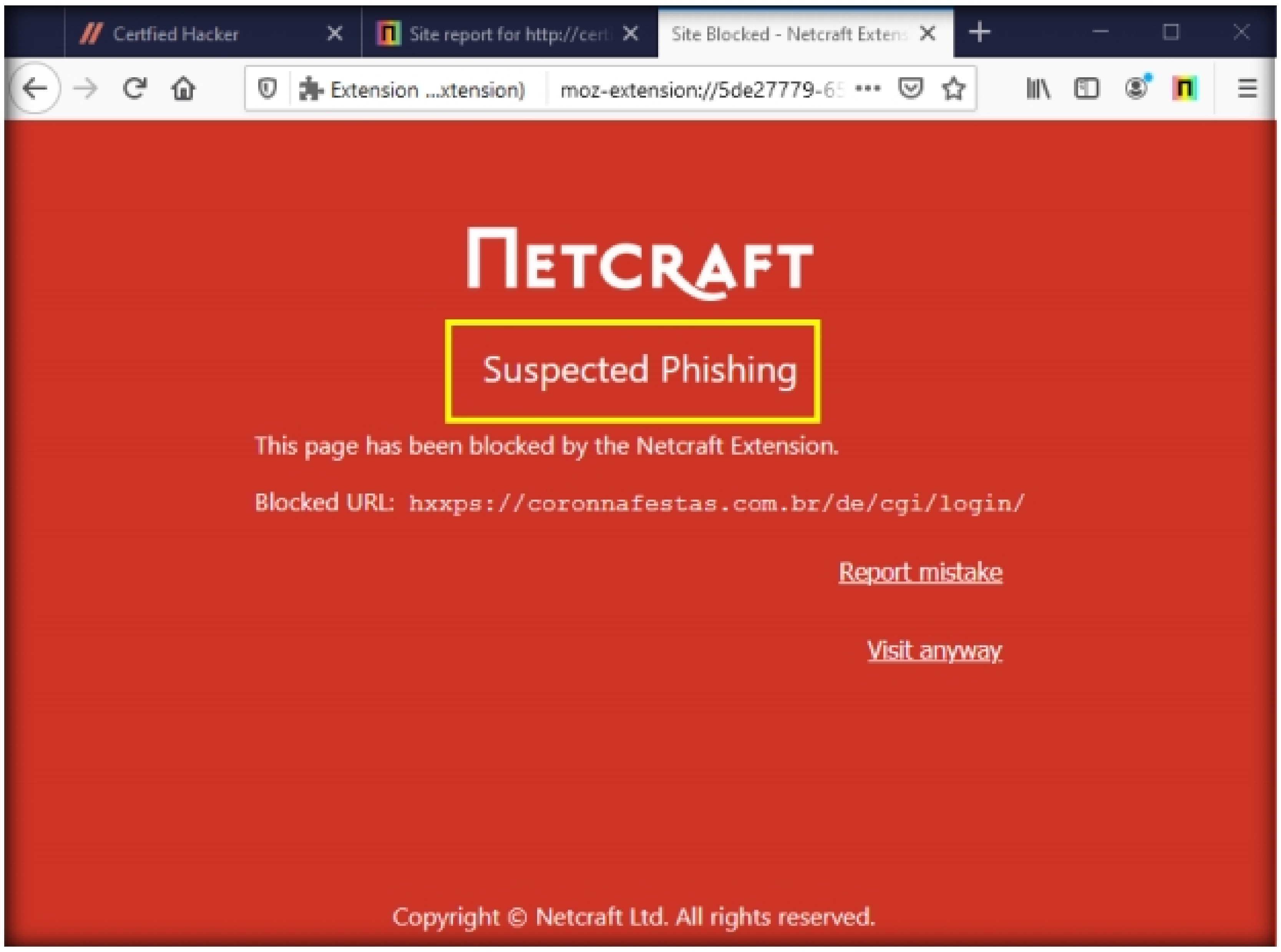
Note: For demonstration purposes, we have used **https://coronnafestas.com.br/de/cgi/login** phishing website to trigger Netcraft Extension to obtain desired results. You can use the same website or any other website to perform this task.

17. The Netcraft Extension automatically blocks phishing sites. However, if you trust the site, click **Visit anyway** to browse it; otherwise, click **Report mistake** to report an incorrectly blocked URL.

Note: If you are getting an error in opening the website (**https://coronnafestas.com.br/de/cgi/login**), try to open other phishing website.

OR

You will get a **Suspected Phishing** page in the **Firefox** browser.



Certfied Hacker
Site report for http://cert
Site Blocked - Netcraft Exten
Extension ...xtension)
moz-extension://5de27779-6
NETCRAFT
Suspected Phishing
Report mistake
Visit anyway

This page has been blocked by the Netcraft Extension.

Blocked URL: `hxxps://coronnafestas.com.br/de/cgi/login/`

Copyright © Netcraft Ltd. All rights reserved.

Figure 2.1.11: Warning pop-up for the blocked site

18. This concludes the demonstration of detecting phishing using Netcraft Extension.

19. Close all open windows and document all the acquired information.

TASK 2

Detect Phishing using PhishTank

In this task, we will use PhishTank to detect phishing.

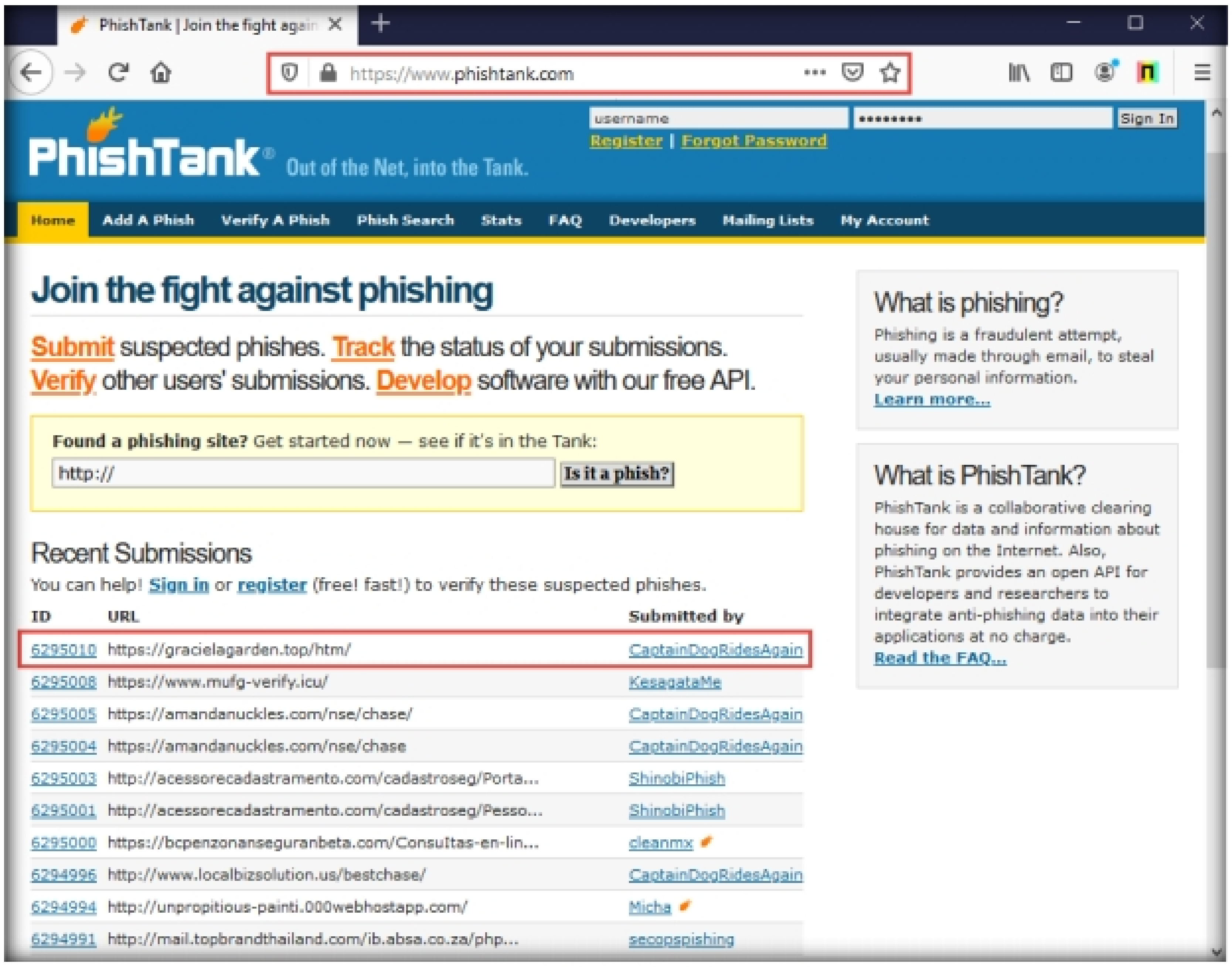
TASK 2.1

Detect Phishing Sites using PhishTank

1. In the **Windows 10** virtual machine, open any web browser (in this case, we are using **Mozilla Firefox**) and go to **https://www.phishtank.com/**.
2. The **PhishTank** webpage appears, displaying a list of phishing websites under **Recent Submissions**.
3. Click on any phishing website **ID** in the **Recent Submissions** list (in this case, **6295010**) to view detailed information about it.

Note: If a notification appears asking **Would you like Firefox to save this login for phishtank.com?**, click **Don't Save**.

PhishTank is a free community site on which anyone can submit, verify, track, and share phishing data. As the official website notes, "it is a collaborative clearing house for data and information about phishing on the Internet." PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications.



Join the fight against phishing

Submit suspected phishes. Track the status of your submissions. Verify other users' submissions. Develop software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

What is phishing?

Phishing is a fraudulent attempt, usually made through email, to steal your personal information.
Learn more...

What is PhishTank?

PhishTank is a collaborative clearing house for data and information about phishing on the Internet. Also, PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge.
Read the FAQ...

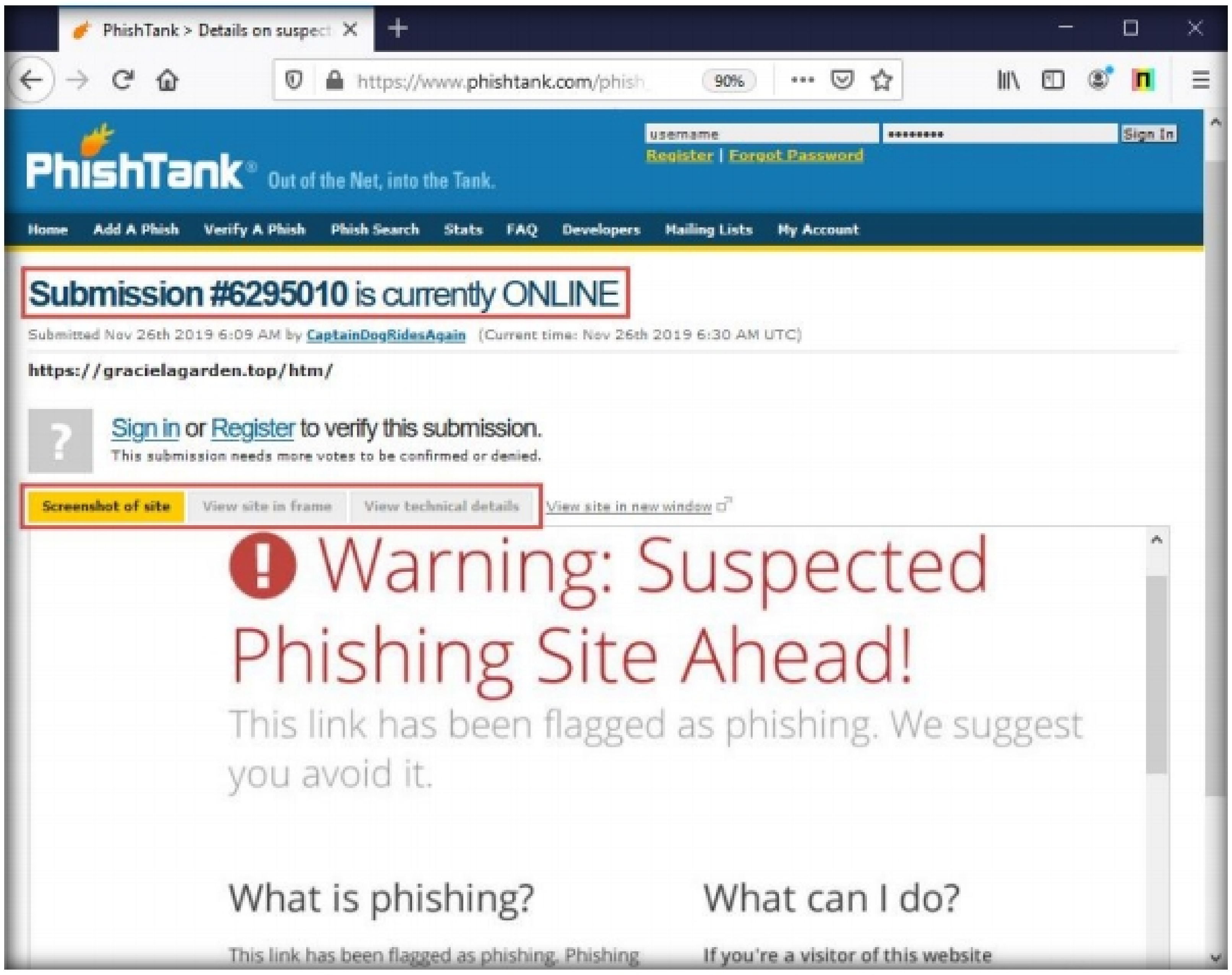
Recent Submissions

You can help! Sign in or register (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
6295010	https://gracielagarden.top/htm/	CaptainDogRidesAgain
6295008	https://www.mufg-verify.icu/	KesagataMe
6295005	https://amandanuckles.com/nse/chase/	CaptainDogRidesAgain
6295004	https://amandanuckles.com/nse/chase	CaptainDogRidesAgain
6295003	http://acessorecadastramento.com/cadastroseg/Porta...	ShinobiPhish
6295001	http://acessorecadastramento.com/cadastroseg/Pesso...	ShinobiPhish
6295000	https://bcpenzonanseguranbeta.com/Consultas-en-lin...	cleanmx
6294996	http://www.localbizsolution.us/bestchase/	CaptainDogRidesAgain
6294994	http://unpropitious-painti.000webhostapp.com/	Micha
6294991	http://mail.topbrandthailand.com/ib.absa.co.za/php...	secopsphishing

Figure 2.2.1: The PhishTank website

4. A page appears displaying information regarding the selected website. You can further view details on the site by navigating to the **View site in frame** and **View technical details** tabs.


PhishTank > Details on suspect
https://www.phishtank.com/phish
90%
PhishTank
Out of the Net, into the Tank.
username
Sign In
Register | Forgot Password
Home
Add A Phish
Verify A Phish
Phish Search
Stats
FAQ
Developers
Mailing Lists
My Account
Screenshot of site
View site in frame
View technical details
View site in new window

Submission #6295010 is currently ONLINE

Submitted Nov 26th 2019 6:09 AM by CaptainDogRidesAgain (Current time: Nov 26th 2019 6:30 AM UTC)

https://gracielagarden.top/htm/

Sign in or Register to verify this submission.

This submission needs more votes to be confirmed or denied.

Warning: Suspected Phishing Site Ahead!

This link has been flagged as phishing. We suggest you avoid it.

What is phishing?

This link has been flagged as phishing. Phishing

What can I do?

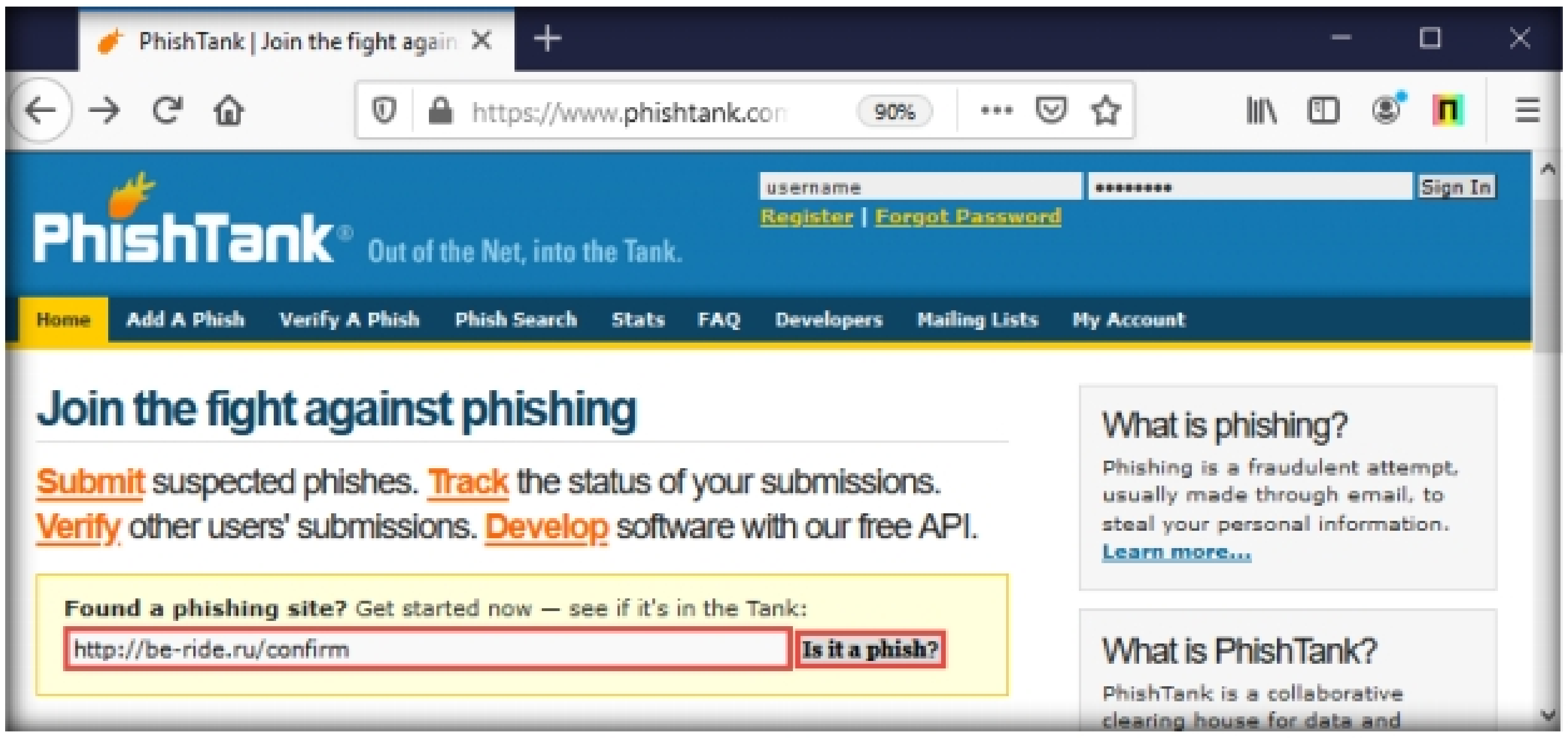
If you're a visitor of this website

Figure 2.2.2: PhishTank information regarding the selected site

5. Navigate back to the **PhishTank** home page by clicking the **Back** button () in the top-left corner of the browser.

6. In the **Found a phishing site?** text field, type a website URL to be checked for phishing (in this example, the URL entered is **be-ride.ru/confirm**). Click the **Is it a phish?** button.

Note: You can examine any website of your choice for phishing.


PhishTank | Join the fight again
https://www.phishtank.com
90%
PhishTank
Out of the Net, into the Tank.
username
Sign In
Register | Forgot Password
Home
Add A Phish
Verify A Phish
Phish Search
Stats
FAQ
Developers
Mailing Lists
My Account
Is it a phish?

Join the fight against phishing

Submit suspected phishes. Track the status of your submissions. Verify other users' submissions. Develop software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

http://be-ride.ru/confirm

What is phishing?

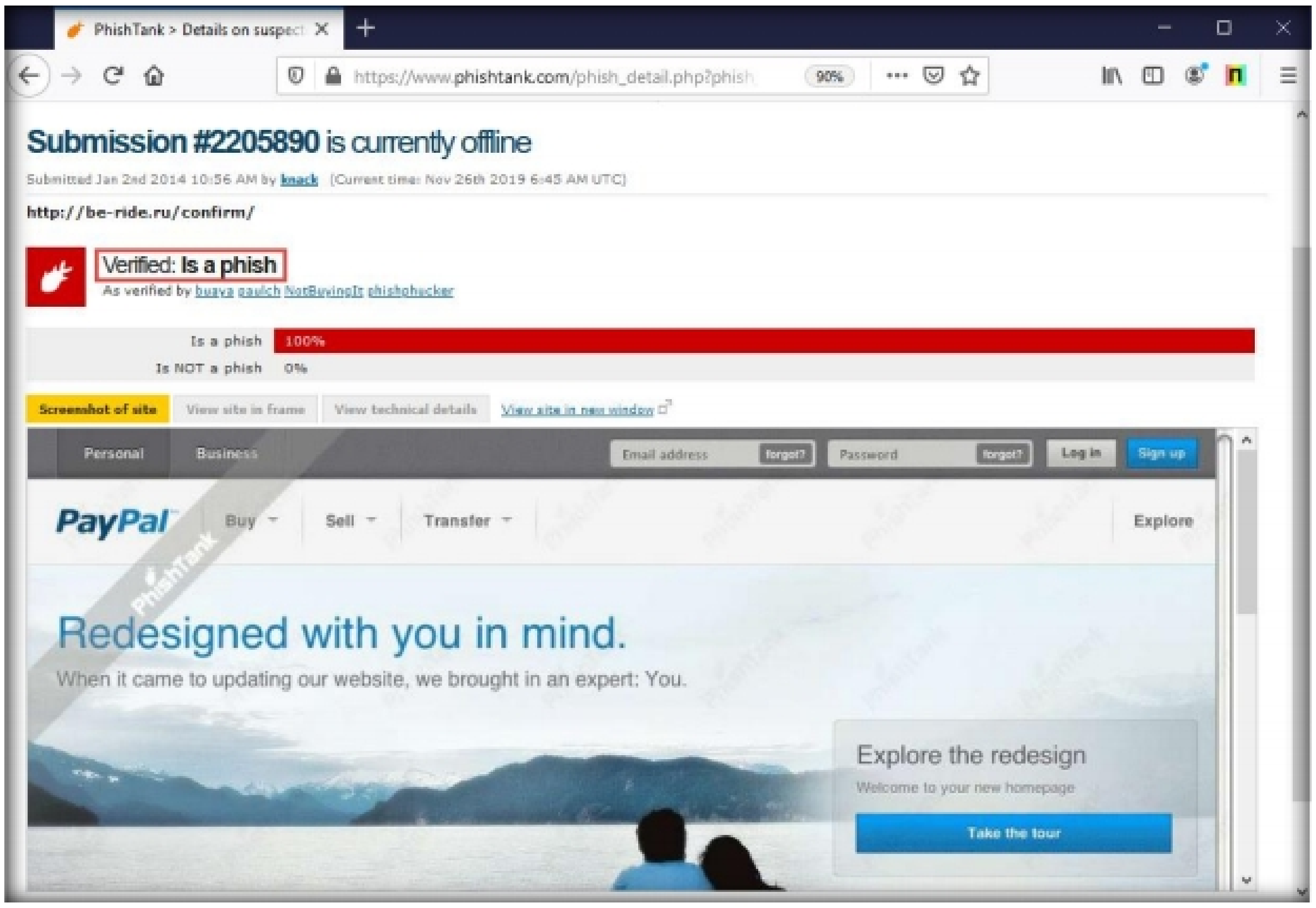
Phishing is a fraudulent attempt, usually made through email, to steal your personal information. Learn more...

What is PhishTank?

PhishTank is a collaborative clearing house for data and

Figure 2.2.3: Checking a site

7. If the site is a phishing site, **PhishTank** returns a result stating that the website "**Is a phish**," as shown in the screenshot.



Submission #2205890 is currently offline

Submitted Jan 2nd 2014 10:56 AM by knack (Current time: Nov 26th 2019 6:45 AM UTC)

http://be-ride.ru/confirm/

Verified: Is a phish

As verified by buaya gaulch NotBuyingIt phishphucker

Is a phish	100%
Is NOT a phish	0%

PhishTank > Details on suspect
https://www.phishtank.com/phish_detail.php?phish
90%
Screenshot of site
View site in frame
View technical details
View site in new window
Personal
Business
Email address
forgot?
Password
forgot?
Log in
Sign up
PayPal
Buy
Sell
Transfer
Explore
PhishTank
Redesigned with you in mind.
When it came to updating our website, we brought in an expert: You.
Explore the redesign
Welcome to your new homepage
Take the tour

Figure: 2.2.4: Phishing website found

8. This concludes the demonstration of detecting phishing using PhishTank.
9. Close all open windows and document all the acquired information.
10. Turn off the **Windows 10** virtual machine.

Lab Analysis

Document the results for all the websites you have checked, and verify whether they are phishing sites.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab

3

Audit Organization's Security for Phishing Attacks

Ethical hackers and penetration testers are aided in auditing an organization's security for phishing attacks by various tools that make security assessment an easy task

ICON KEY

- 🗀 Valuable information
- ✎ Test your knowledge
- 💻 Web exercise
- 📖 Workbook review

Lab Scenario

Social engineers exploit human behavior (manners, enthusiasm toward work, laziness, innocence, etc.) to gain access to the information resources of the target company. This information is difficult to be guarded against social engineering attacks, as the victim may not be aware that he or she has been deceived. The attacks performed are similar to those used to extract a company's valuable data. To guard against social engineering attacks, a company must evaluate the risk of different types of attacks, estimate the possible losses, and spread awareness among its employees.

As a professional ethical hacker or pen tester, you must perform phishing attacks in the organization to assess the awareness of its employees.

🗀 **Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 09 Social Engineering**

As an administrator or penetration tester, you may have implemented highly sophisticated and expensive technology solutions; however, all these techniques can be bypassed if the employees fall prey to simple social engineering scams. Thus, employees must be educated about the best practices for protecting the organization's systems and information.

In this lab, you will learn how to audit an organization's security for phishing attacks within the organization.

Lab Objectives

- Audit organization's security for phishing attacks using OhPhish

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine

- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview

In phishing attacks, attackers implement social engineering techniques to trick employees into revealing confidential information of their organization. They use social engineering to commit fraud, identity theft, industrial espionage, and so on. To guard against social engineering attacks, organizations must develop effective policies and procedures; however, merely developing them is not enough.

To be truly effective in combating social engineering attacks, an organization should do the following:

- Disseminate policies among its employees and provide proper education and training.
- Provide specialized training benefits to employees who are at a high risk of social engineering attacks.
- Obtain signatures of employees on a statement acknowledging that they understand the policies.
- Define the consequences of policy violations.

Lab Tasks

TASK 1

Audit Organization's Security for Phishing Attacks using OhPhish

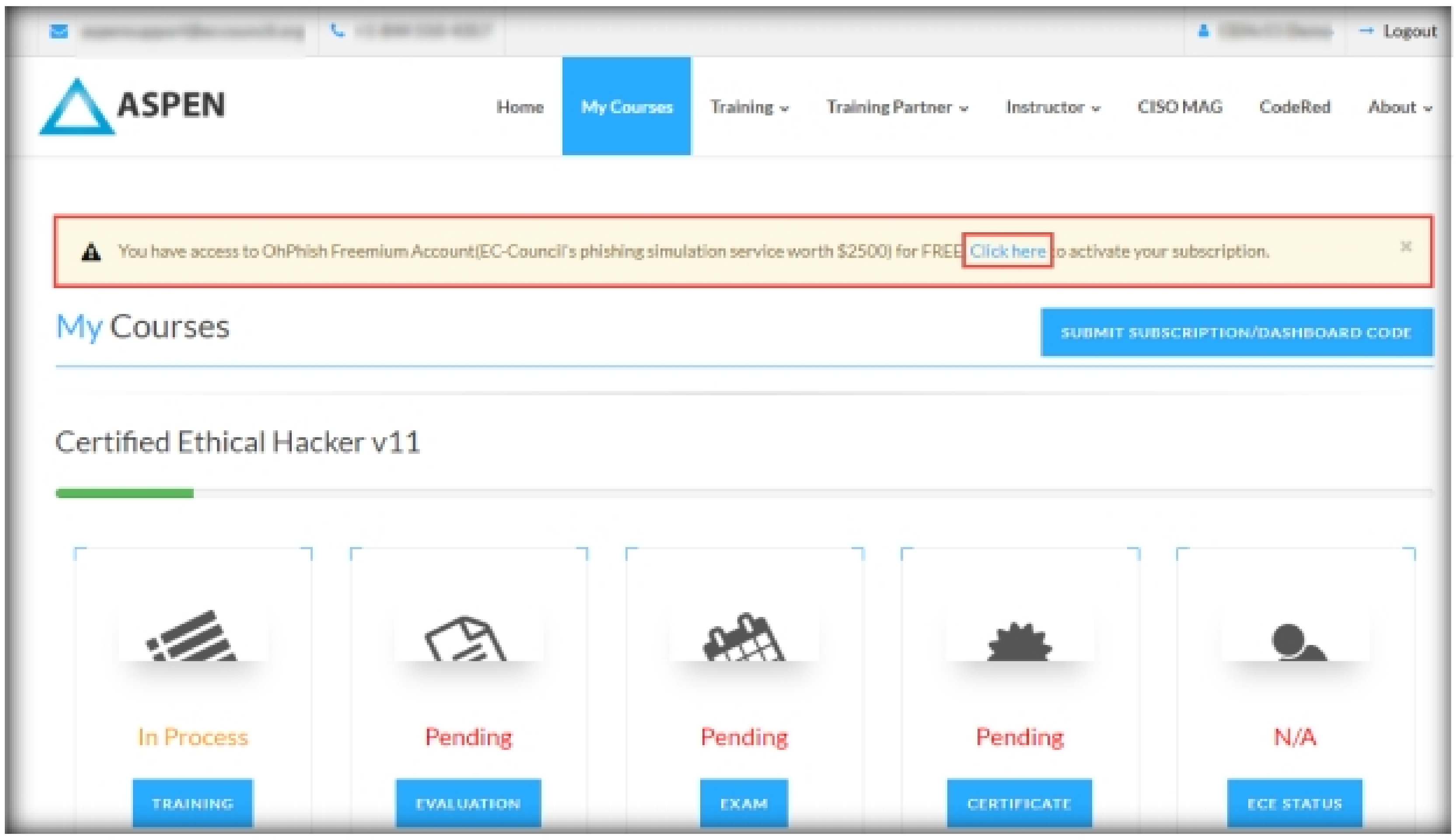
Here, we will audit the organization's security infrastructure for phishing attacks using OhPhish.

1. Turn on the **Windows 10** virtual machine and login with the credentials **Admin** and **Pa$$w0rd**.

TASK 1.1

Activate OhPhish Account

2. Before starting this task, you must activate your **OhPhish** account.
3. Open any web browser (here, **Mozilla Firefox**). Log in to your **ASPEN** account and navigate to **Certified Ethical Hacker v11** in the **My Courses** section.
4. Click on **Click here** hyperlink in the **OhPhish** notification above **My Courses** section.


[redacted] [redacted] [redacted] Logout
ASPEN
Home
My Courses
Training
Training Partner
Instructor
CISO MAG
CodeRed
About
SUBMIT SUBSCRIPTION/DASHBOARD CODE
TRAINING
EVALUATION
EXAM
CERTIFICATE
ECE STATUS

You have access to OhPhish Freemium Account(EC-Council's phishing simulation service worth $2500) for FREE Click here to activate your subscription.

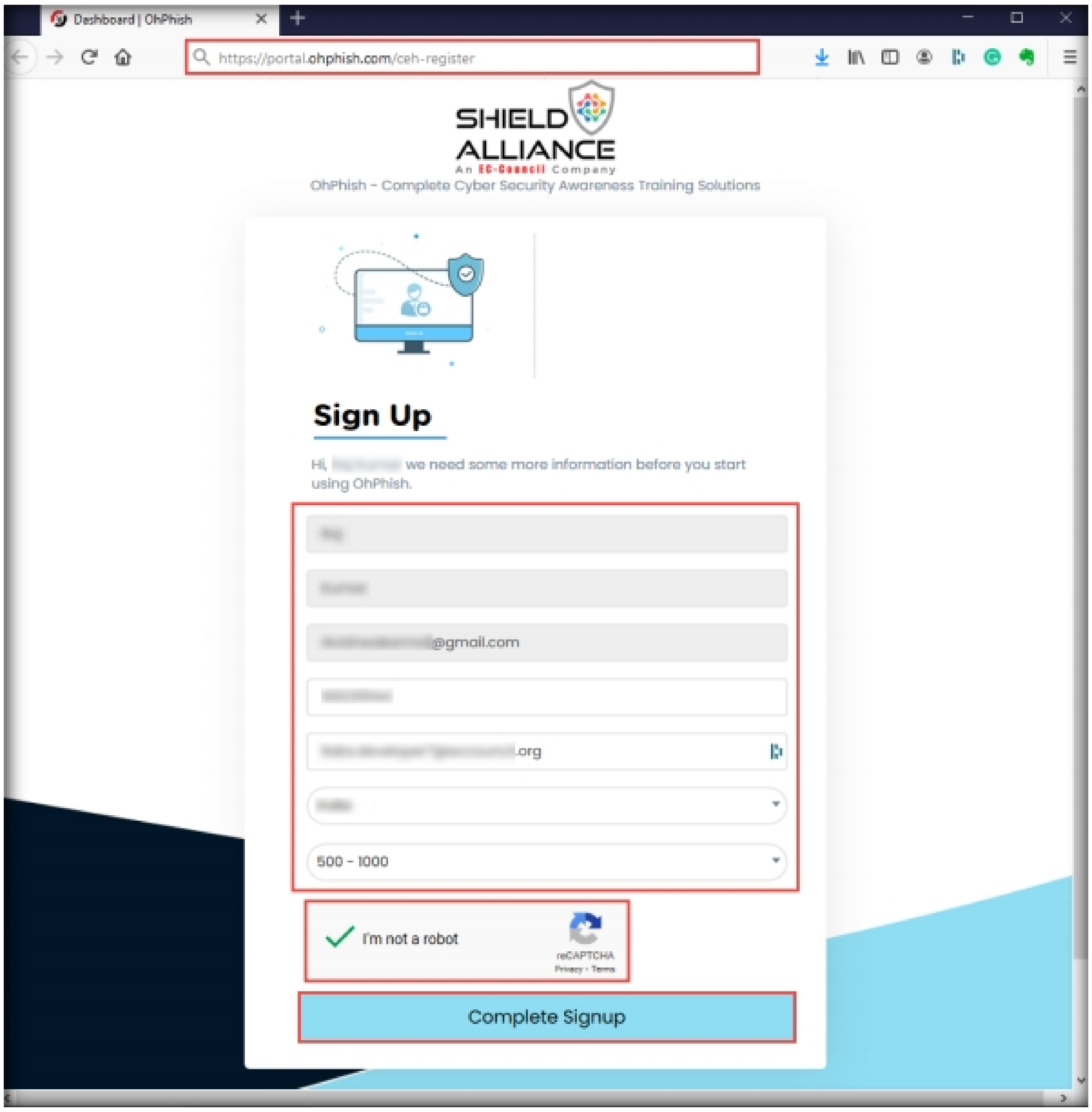
My Courses

Certified Ethical Hacker v11

TRAINING	EVALUATION	EXAM	CERTIFICATE	ECE STATUS
In Process	Pending	Pending	Pending	N/A

Figure 3.1.1: ASPEN account – click on Click here

5. You will be redirected to the OhPhish **Sign Up** page. Enter the personal details, check **I'm not a robot** checkbox and click **Complete Signup** button.


Dashboard | OhPhish
SHIELD ALLIANCE
An EC-Council Company
OhPhish - Complete Cyber Security Awareness Training Solutions
Sign Up
I'm not a robot
reCAPTCHA
Privacy - Terms
Complete Signup

https://portal.ohphish.com/ceh-register

Hi, [redacted] we need some more information before you start using OhPhish.

[redacted]

[redacted]

[redacted]@gmail.com

[redacted]

[redacted].org

[redacted]

500 - 1000

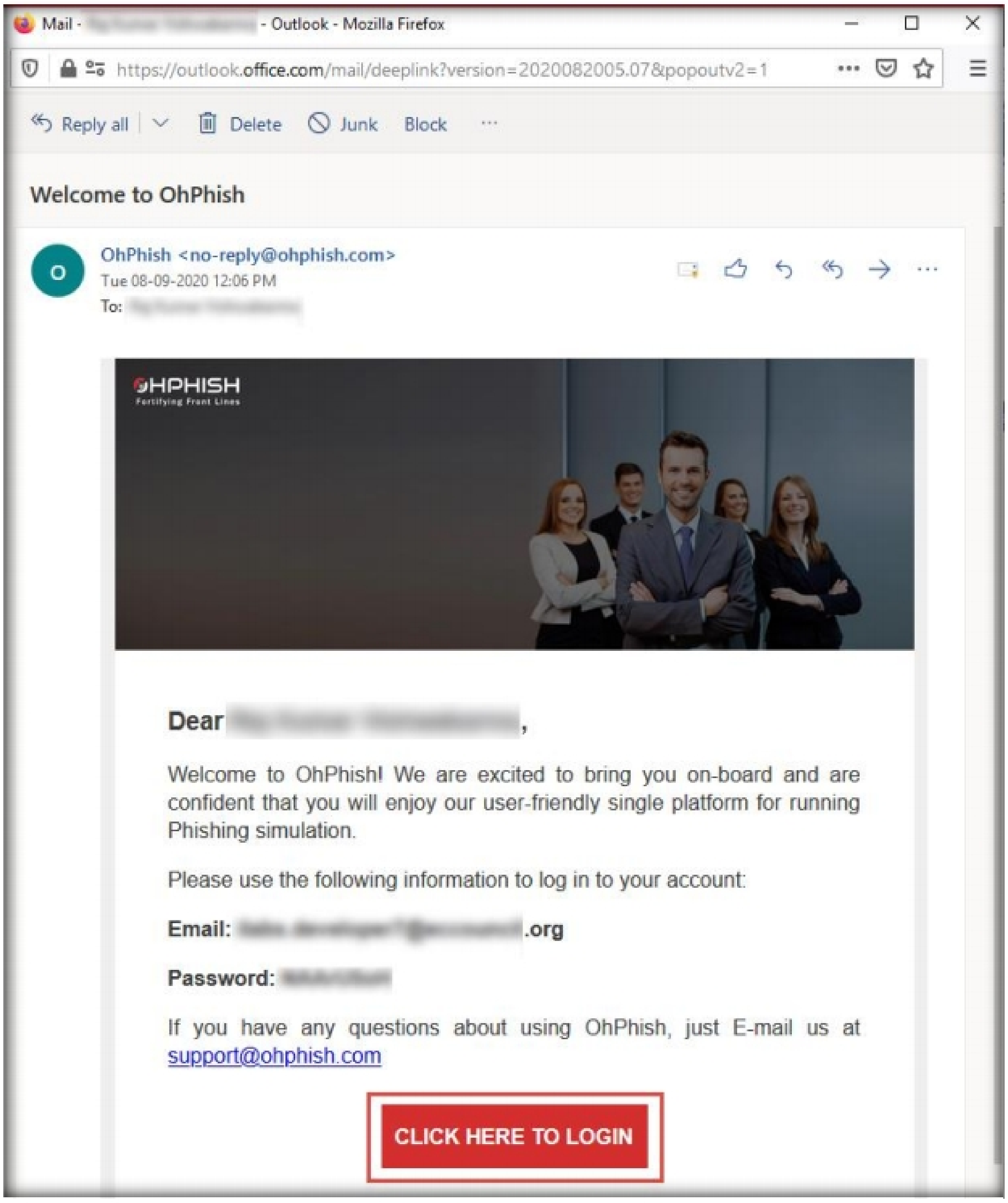
☑ I'm not a robot

Figure 3.1.2: OhPhish Sign Up

6. Account creation **Alert!** appears, click **OK**.

7. Now, open your email account given during registration process. Open an email from **OhPhish** and in the email, click **CLICK HERE TO LOGIN** button.

OhPhish is a web-based portal for testing employees' susceptibility to social engineering attacks. It is a phishing simulation tool that provides an organization with a platform to launch phishing simulation campaigns on its employees.


Mail - [redacted] - Outlook - Mozilla Firefox
https://outlook.office.com/mail/deeplink?version=2020082005.07&popoutv2=1
Reply all
Delete
Junk
Block
OHPHISH
Fortifying Front Lines
CLICK HERE TO LOGIN

Welcome to OhPhish

OhPhish <no-reply@ohphish.com>
Tue 08-09-2020 12:06 PM
To: [redacted]

Dear [redacted],

Welcome to OhPhish! We are excited to bring you on-board and are confident that you will enjoy our user-friendly single platform for running Phishing simulation.

Please use the following information to log in to your account:

Email: [redacted].org

Password: [redacted]

If you have any questions about using OhPhish, just E-mail us at support@ohphish.com

Figure 3.1.3: OhPhish email

8. **OhPhish** login page appears, log in using the credentials received in the email.

Note: If **Would you like Firefox to save this login for ohphish.com?** notification appears, click **Don't Save**.

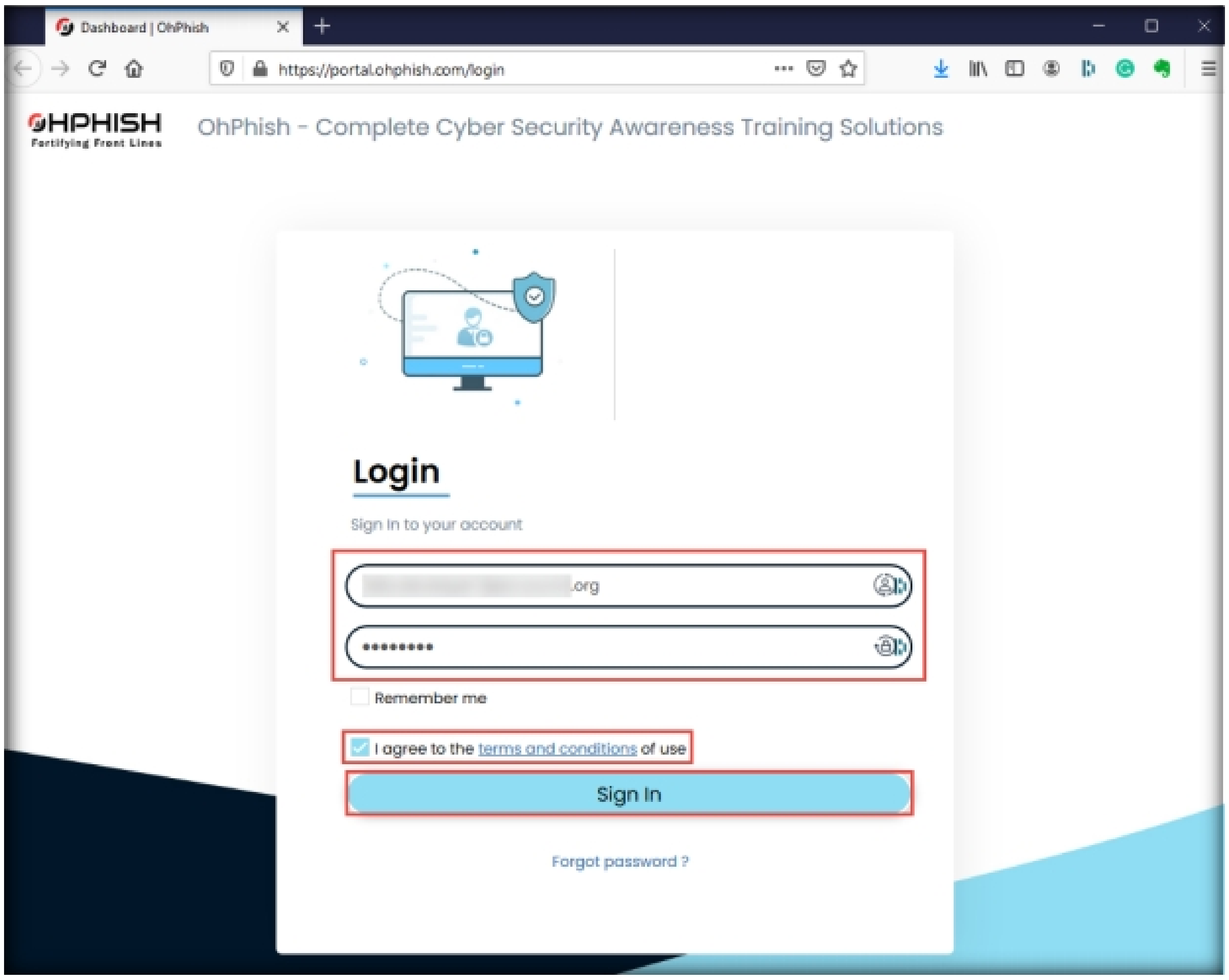

Dashboard | OhPhish
https://portal.ohphish.com/login
OHPHISH
Fortifying Front Lines
OhPhish - Complete Cyber Security Awareness Training Solutions
Login
Sign in to your account
.org
••••••••
Remember me
I agree to the terms and conditions of use
Sign In
Forgot password ?

Figure 3.1.4: OhPhish login page

9. You will be redirected to **Reset Password** page, enter the new password in both the fields and click **Reset Password** button to reset the password.

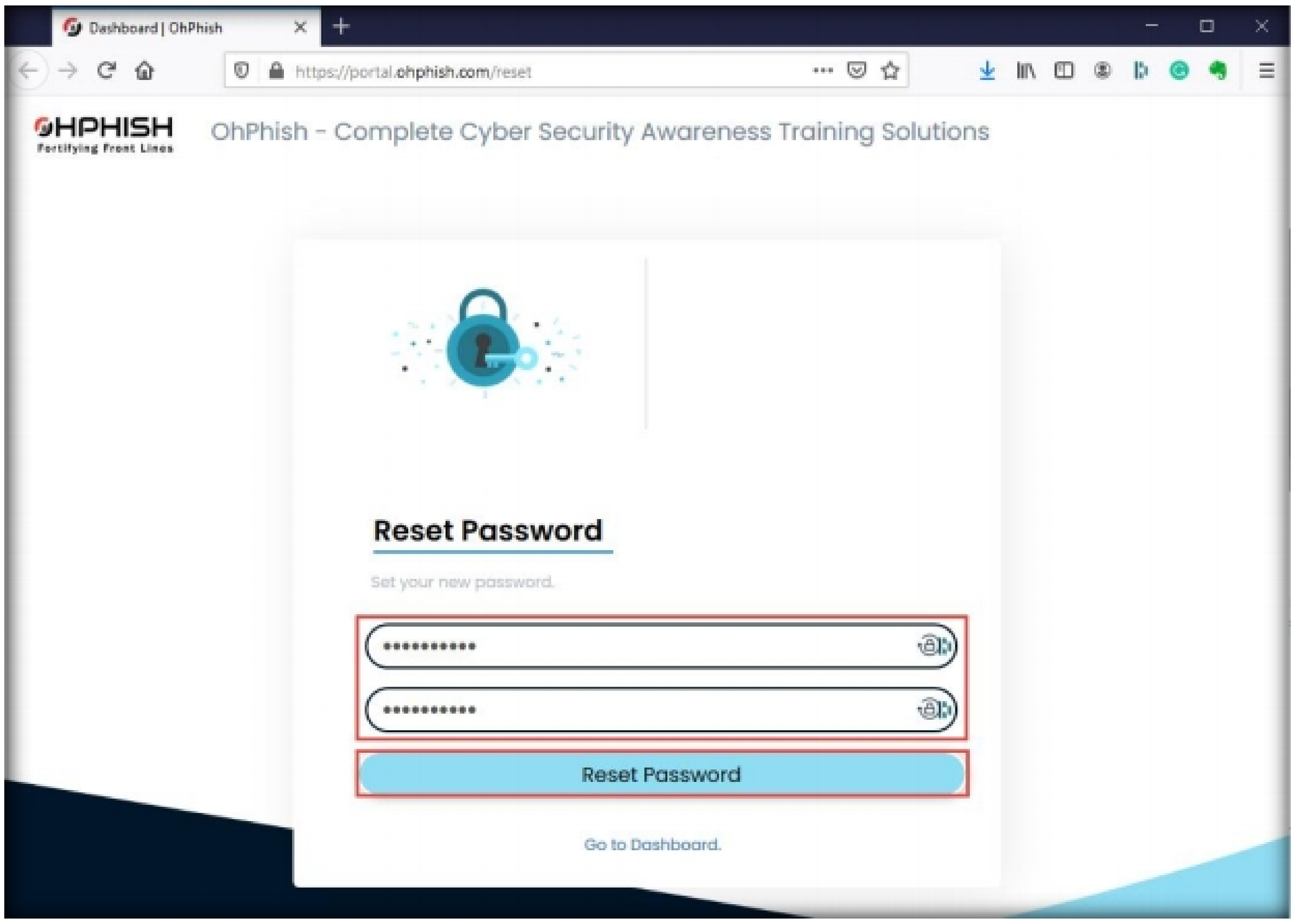

Dashboard | OhPhish
https://portal.ohphish.com/reset
OHPHISH
Fortifying Front Lines
OhPhish - Complete Cyber Security Awareness Training Solutions
Reset Password
Set your new password.
•••••••••••
•••••••••••
Reset Password
Go to Dashboard.

Figure 3.1.5: Reset Password

10. Your account password is changed successfully.

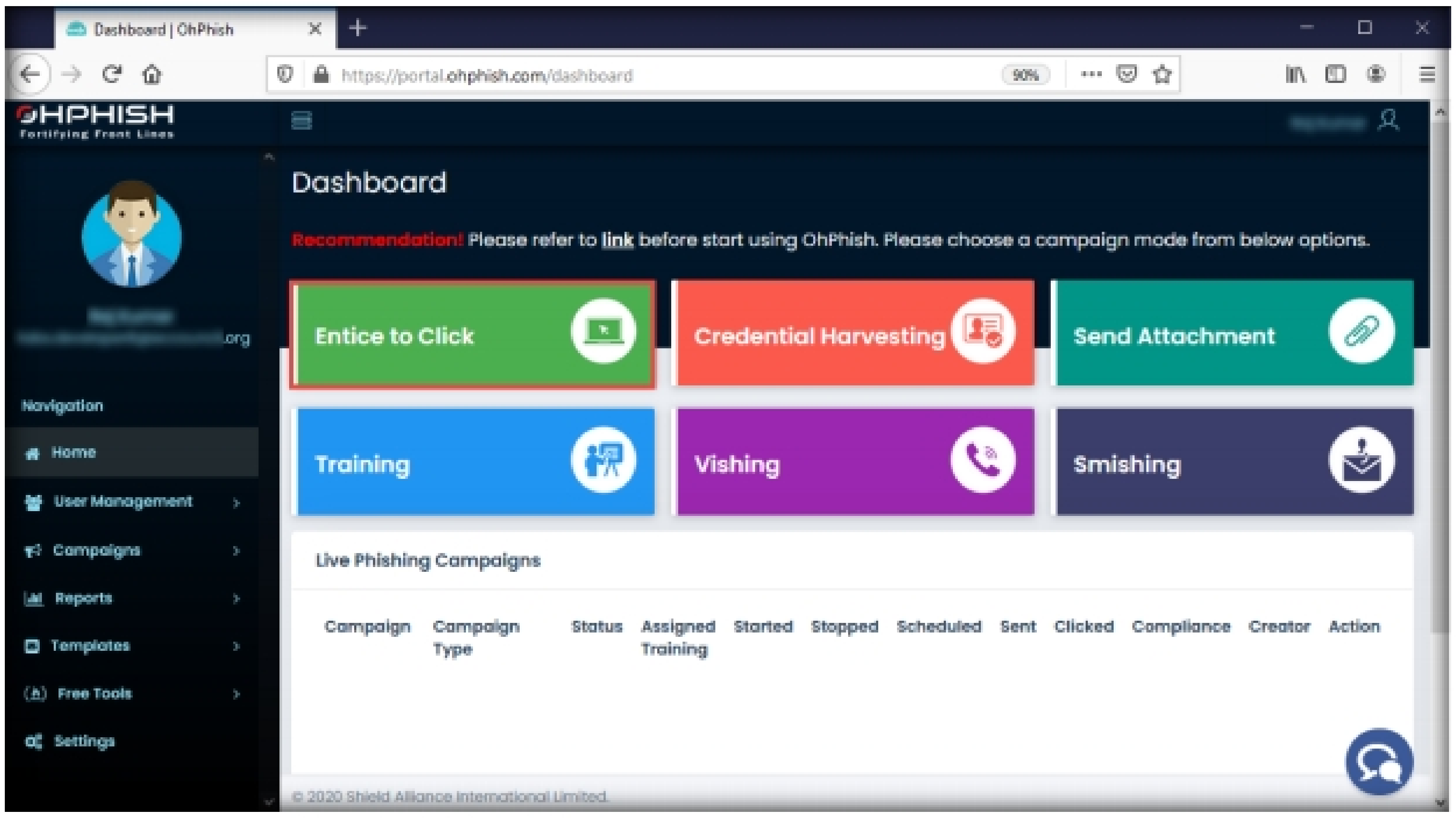
11. Now, you can login to your OhPhish account either by clicking on the **LOGIN TO OHPHISH PORTAL** button in your **ASPEN** account under **My Courses** section or you can navigate to the **OhPhish** website (**https://portal.ohphish.com/login**) and login using your credentials.

TASK 1.2

Phish using Entice to Click

12. Once login to your OhPhish account, you will be redirected to the OhPhish **Dashboard**.

13. In the OhPhish **Dashboard**, click on the **Entice to Click** option.


Dashboard | OhPhish
https://portal.ohphish.com/dashboard
90%
OHPHISH
Fortifying Front Lines
Navigation
Home
User Management
Campaigns
Reports
Templates
Free Tools
Settings
Dashboard
Entice to Click
Credential Harvesting
Send Attachment
Training
Vishing
Smishing
Live Phishing Campaigns
Campaign
Campaign Type
Status
Assigned Training
Started
Stopped
Scheduled
Sent
Clicked
Compliance
Creator
Action
© 2020 Shield Alliance International Limited.

Recommendation! Please refer to link before start using OhPhish. Please choose a campaign mode from below options.

Figure 3.1.6: OhPhish Dashboard – Select Entice to Click

The OhPhish platform captures the responses and provides MIS reports and trends (on a real-time basis) that can be tracked according to the user, department, or designation.

14. The **Create New Email Phishing Campaign** form appears.

Note: If the **OhPhish Helpdesk** notification appears in the right corner of the dashboard, close it.

15. In the **Campaign Name** field, enter any name (here, **Test - Entice to Click**). In the **Select Template Category** field, select **Coronavirus/COVID-19** from the drop-down list.

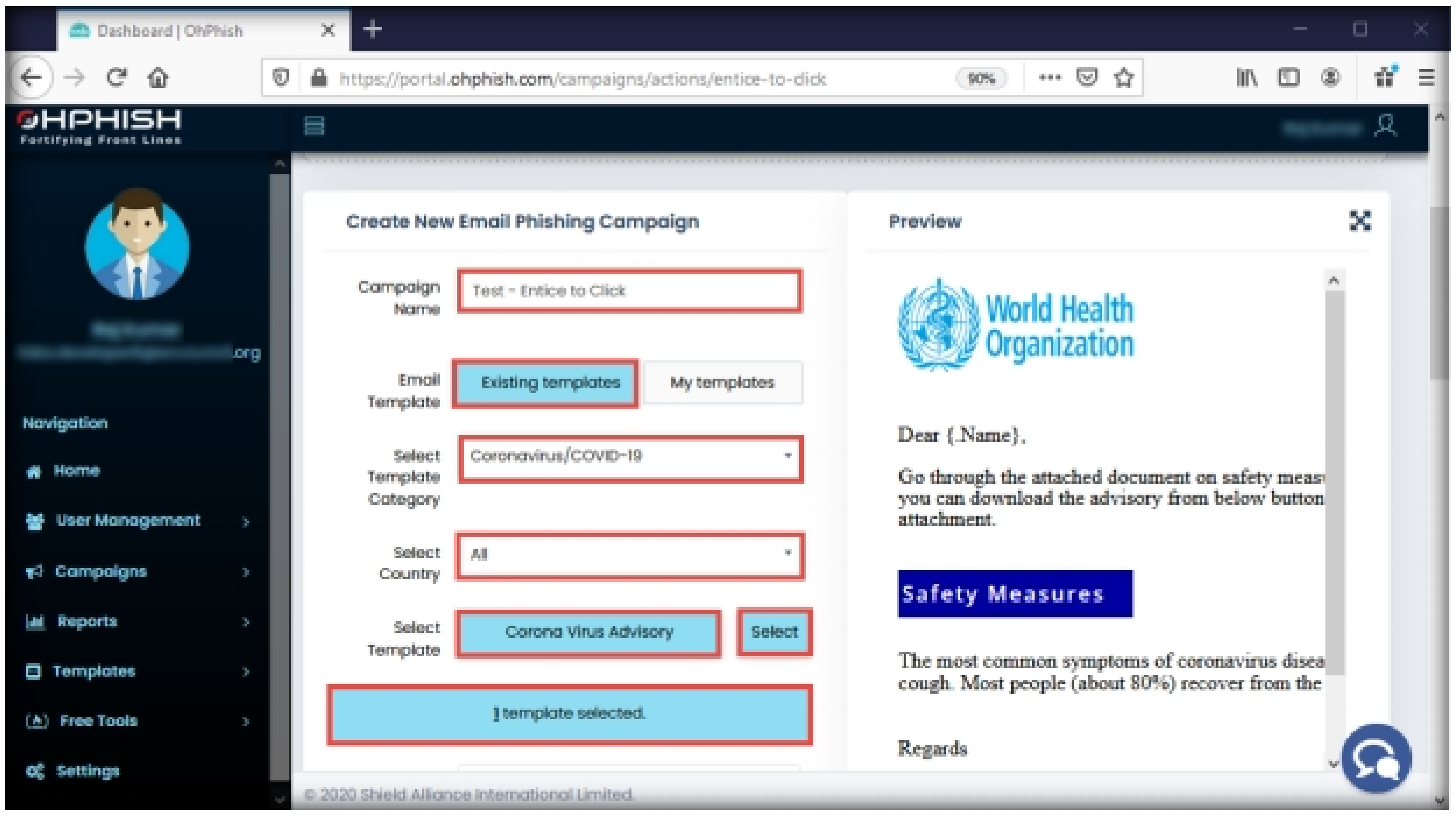
Note: Ensure that the **Existing Template** is selected in the **Email Template** option.

16. In the **Select Country** field, leave the default option selected (**All**).

17. In the **Select Template** field, click the **Select Template** button and select **Corona Virus Advisory** from the drop-down list.

18. Click the **Select** button in the **Select Template** field to select the template.

Note: The **template selected** notification appears below the **Select Template** field.


Dashboard | OhPhish
https://portal.ohphish.com/campaigns/actions/entice-to-click
90%
OHPHISH
Fortifying Front Lines
[redacted]
Navigation
Home
User Management
Campaigns
Reports
Templates
Free Tools
Settings
Preview
© 2020 Shield Alliance International Limited.

Create New Email Phishing Campaign

Campaign Name: Test - Entice to Click

Email Template: Existing templates | My templates

Select Template Category: Coronavirus/COVID-19

Select Country: All

Select Template: Corona Virus Advisory | Select

1 template selected.

World Health Organization

Dear {.Name},

Go through the attached document on safety meas
you can download the advisory from below button
attachment.

Safety Measures

The most common symptoms of coronavirus disea
cough. Most people (about 80%) recover from the

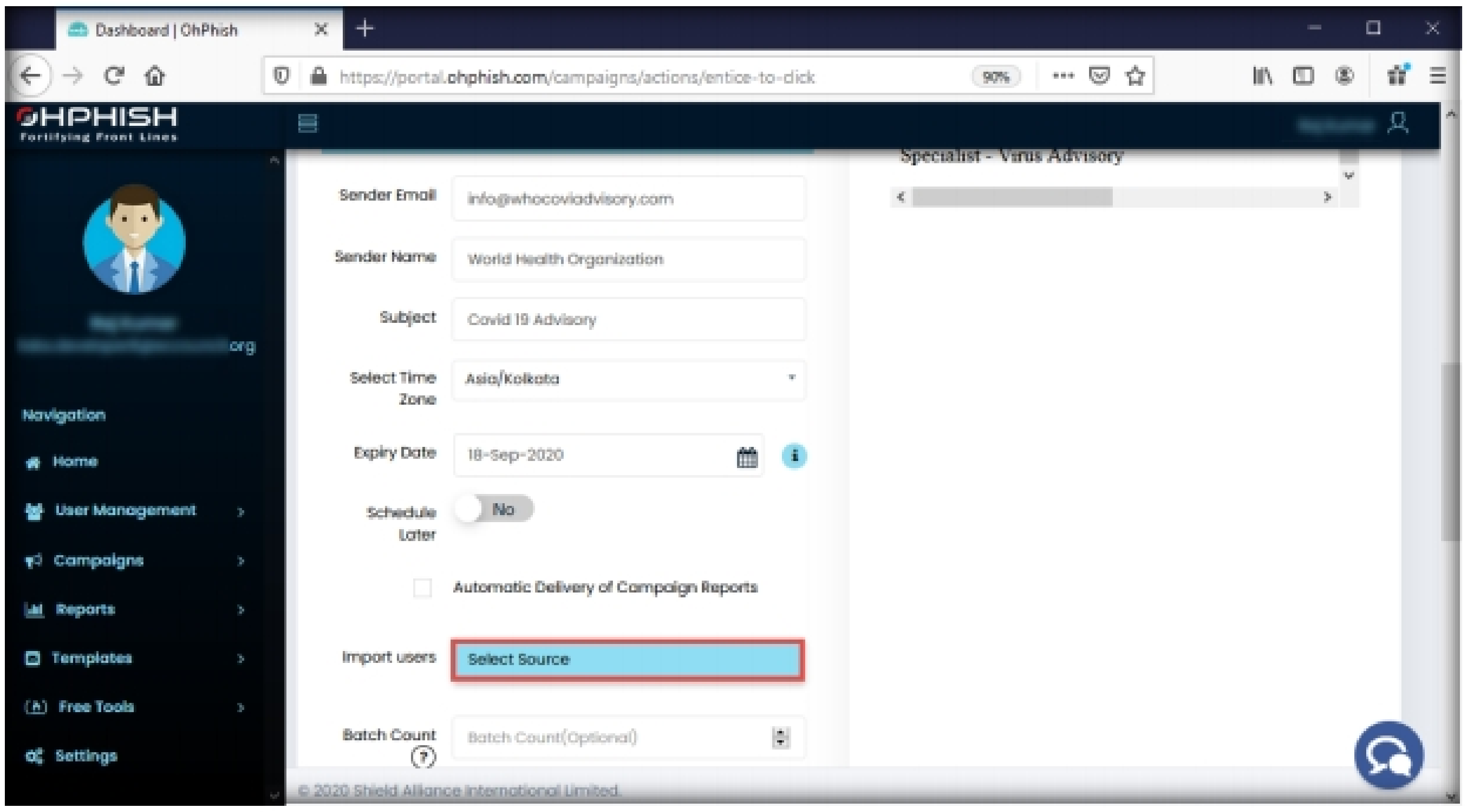
Regards

Figure 3.1.7: Create New Email Phishing Campaign form

19. Leave fields such as **Sender Email**, **Sender Name**, **Subject**, **Select Time Zone**, **Expiry Date**, and **Schedule Later** set to their default values, as shown in the screenshot.

Note: You can change the above-mentioned options if you want to.

20. In the **Import users** field, click **Select Source**.


Dashboard | OhPhish
https://portal.ohphish.com/campaigns/actions/entice-to-click
90%
OHPHISH
Fortifying Front Lines
[redacted]
Navigation
Home
User Management
Campaigns
Reports
Templates
Free Tools
Settings
Specialist - Virus Advisory
© 2020 Shield Alliance International Limited.

Sender Email: info@whocoviadvisory.com

Sender Name: World Health Organization

Subject: Covid 19 Advisory

Select Time Zone: Asia/Kolkata

Expiry Date: 18-Sep-2020

Schedule Later: No

☐ Automatic Delivery of Campaign Reports

Import users: Select Source

Batch Count: Batch Count(Optional)

Figure 3.1.8: Create New Email Phishing Campaign form

21. **Import Users** pop-up appears, click to select **Quick Add** option from the list of options.

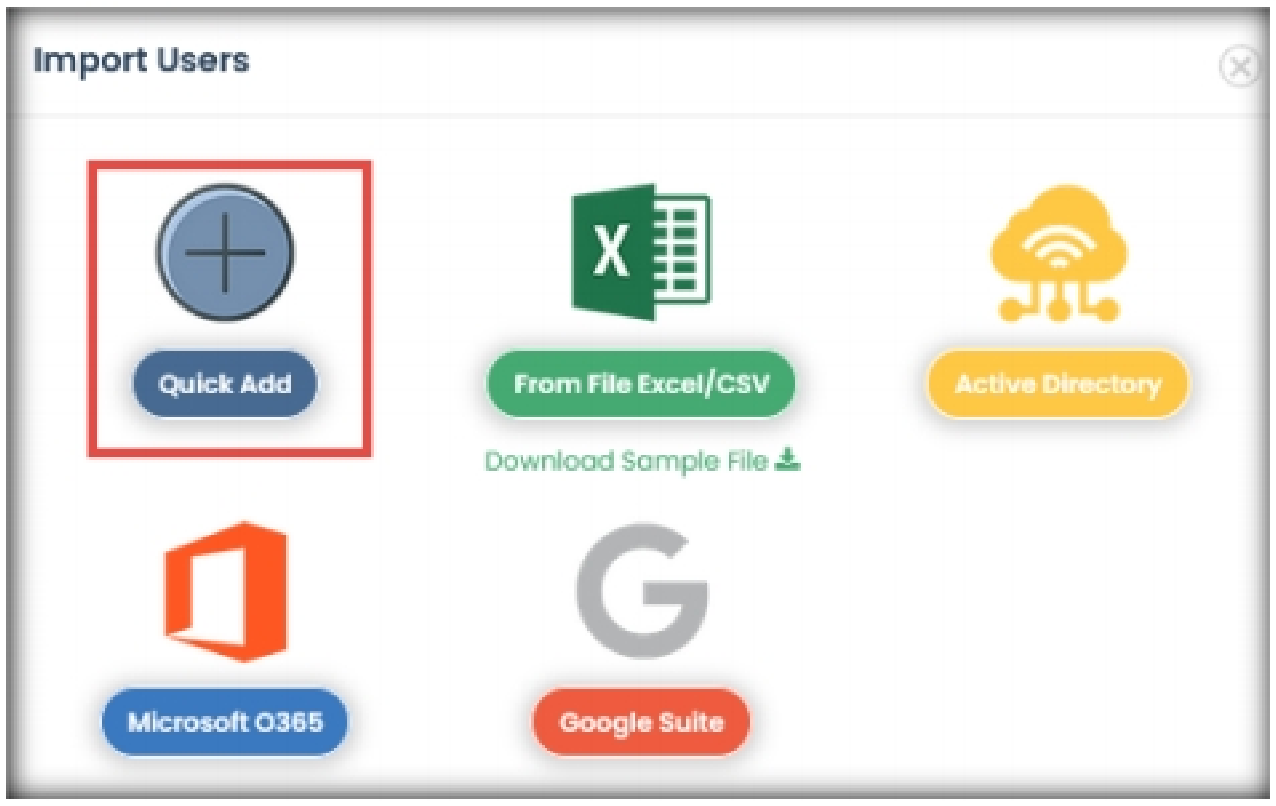

Import Users
Quick Add
From File Excel/CSV
Download Sample File
Active Directory
Microsoft O365
Google Suite

Figure 3.1.9: Import Users pop-up

22. The **Import Users Info** pop-up appears; enter the details of the employee and click **Add**.

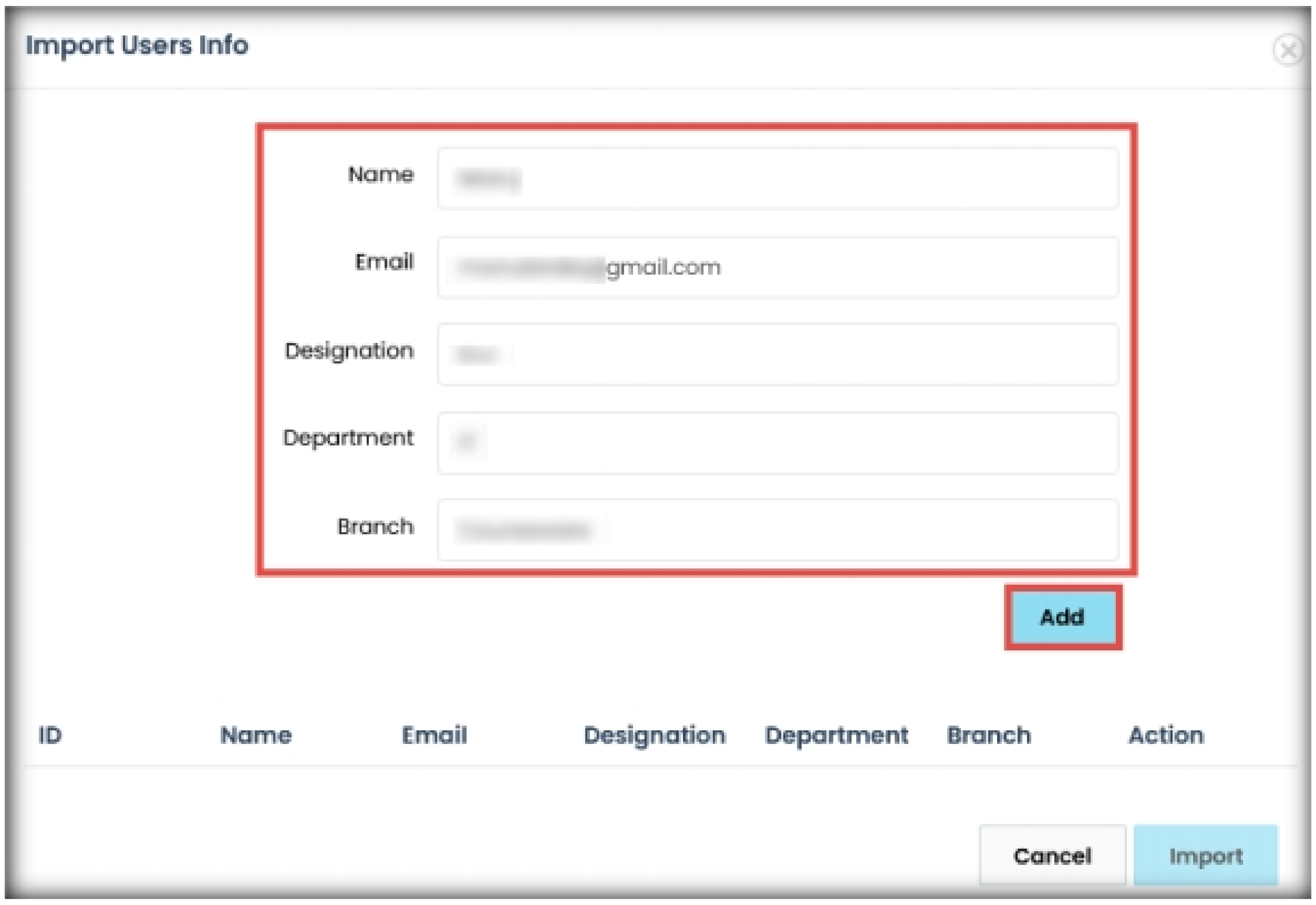

Import Users Info
Name
Email
Designation
Department
Branch
Add
ID
Name
Email
Designation
Department
Branch
Action
Cancel
Import

Figure 3.1.10: Import Users Info

23. Similarly, you can add the details of multiple users. Here, we added two users.

24. After adding the users' details, click **Import**.

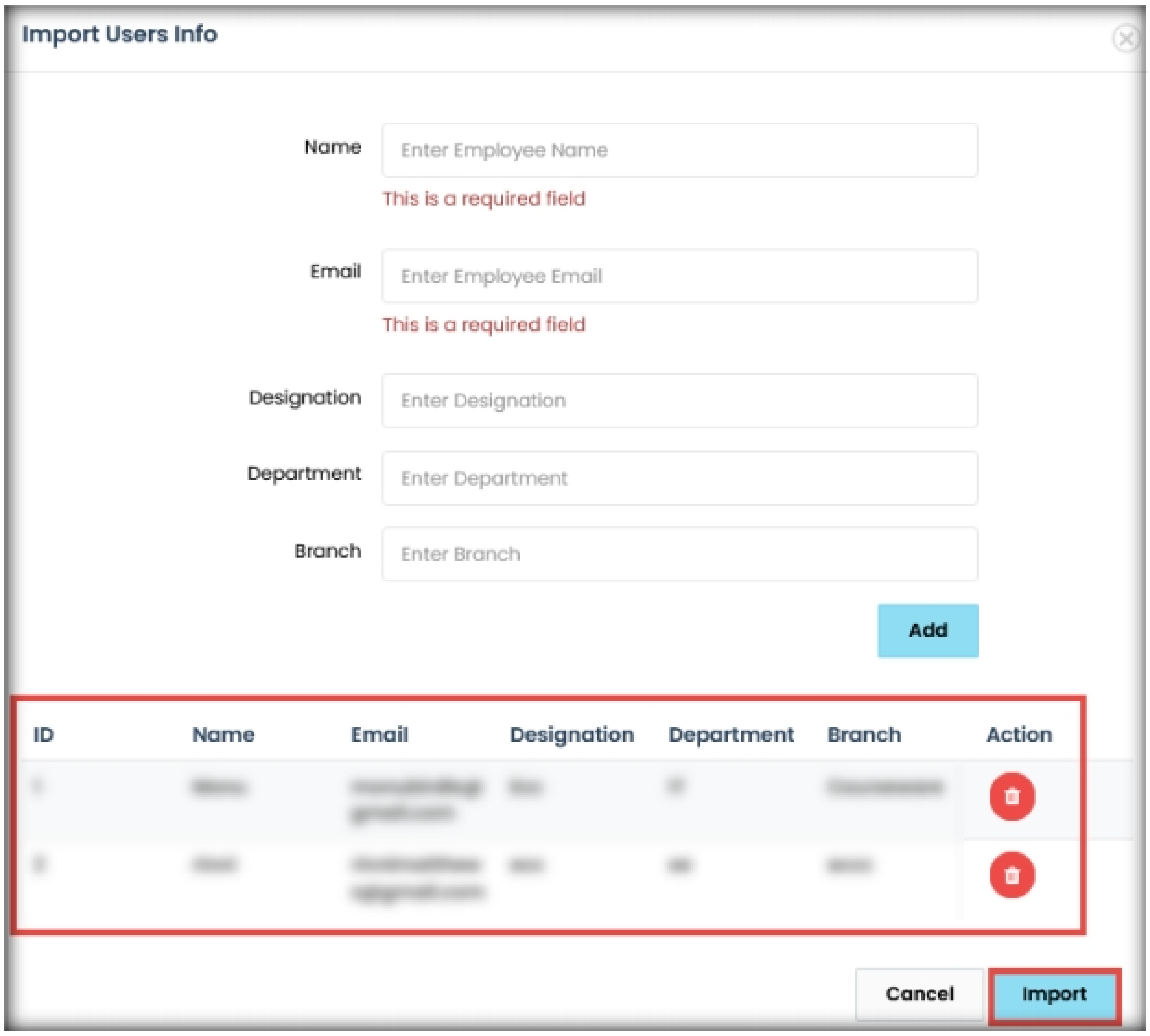

Import Users Info
Name
Enter Employee Name
This is a required field
Email
Enter Employee Email
This is a required field
Designation
Enter Designation
Department
Enter Department
Branch
Enter Branch
Add
ID
Name
Email
Designation
Department
Branch
Action
Cancel
Import

Figure 3.1.11: Click Import to add users

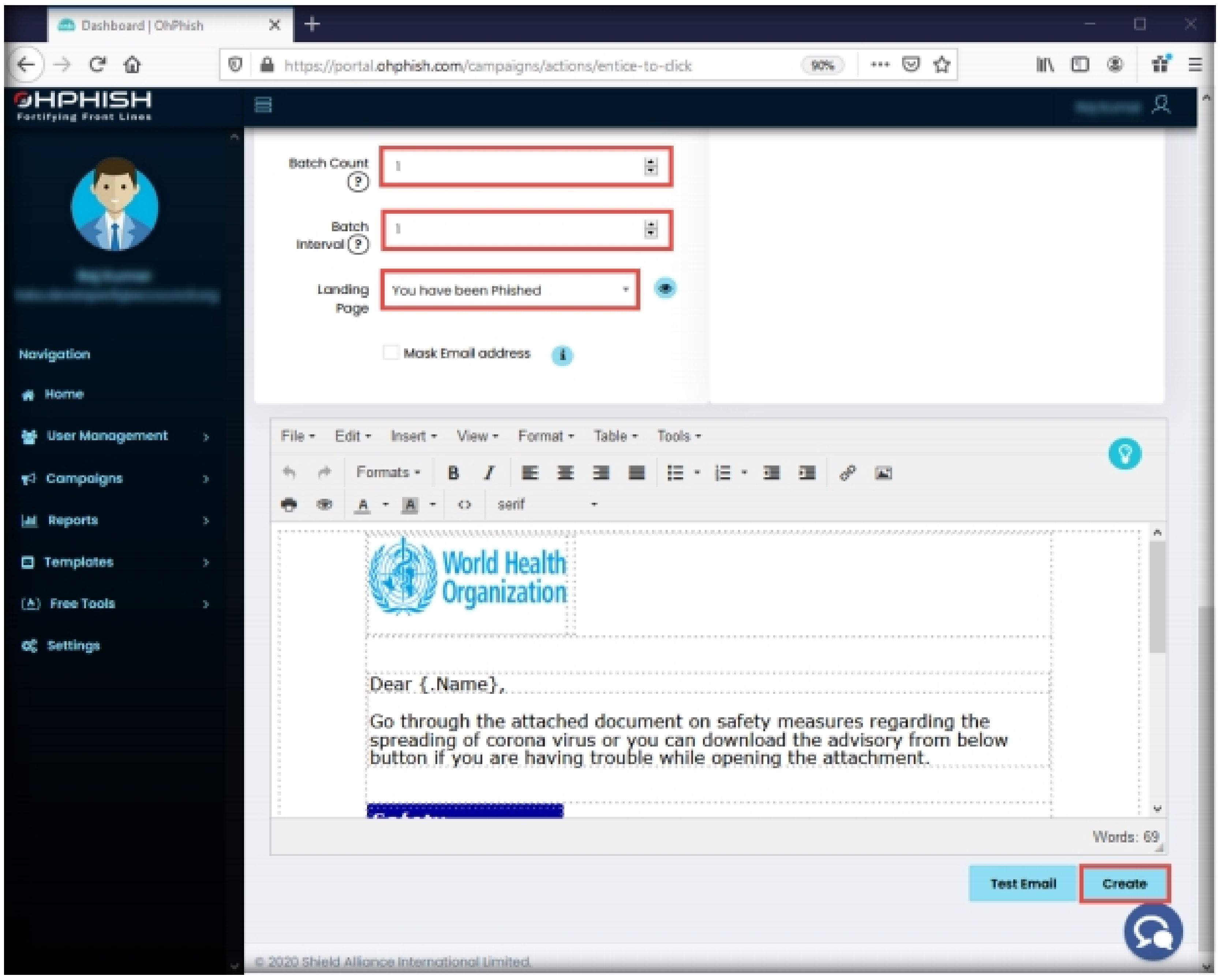
25. In the **Batch Count** and **Batch Interval** fields, set the values to **1**.

Note: **Batch Count**: indicates how many you want to send emails to at one time; **Batch Interval**: indicates at what interval (in minutes) you want to send emails to a batch of users.

Note: The values of **Batch Count** and **Batch Interval** might differ depending on the number of users you are sending phishing emails to.

26. Leave the **Landing Page** field set to its default value.

27. Now, scroll down to the end of the page and click **Create** to create the phishing campaign.


Dashboard | OhPhish
https://portal.ohphish.com/campaigns/actions/entice-to-click
OHPHISH
Fortifying Front Lines
Navigation
Home
User Management
Campaigns
Reports
Templates
Free Tools
Settings
File Edit Insert View Format Table Tools
Formats
serif
World Health Organization
Words: 69
Test Email
Create
© 2020 Shield Alliance International Limited.

Batch Count: 1

Batch Interval: 1

Landing Page: You have been Phished

☐ Mask Email address

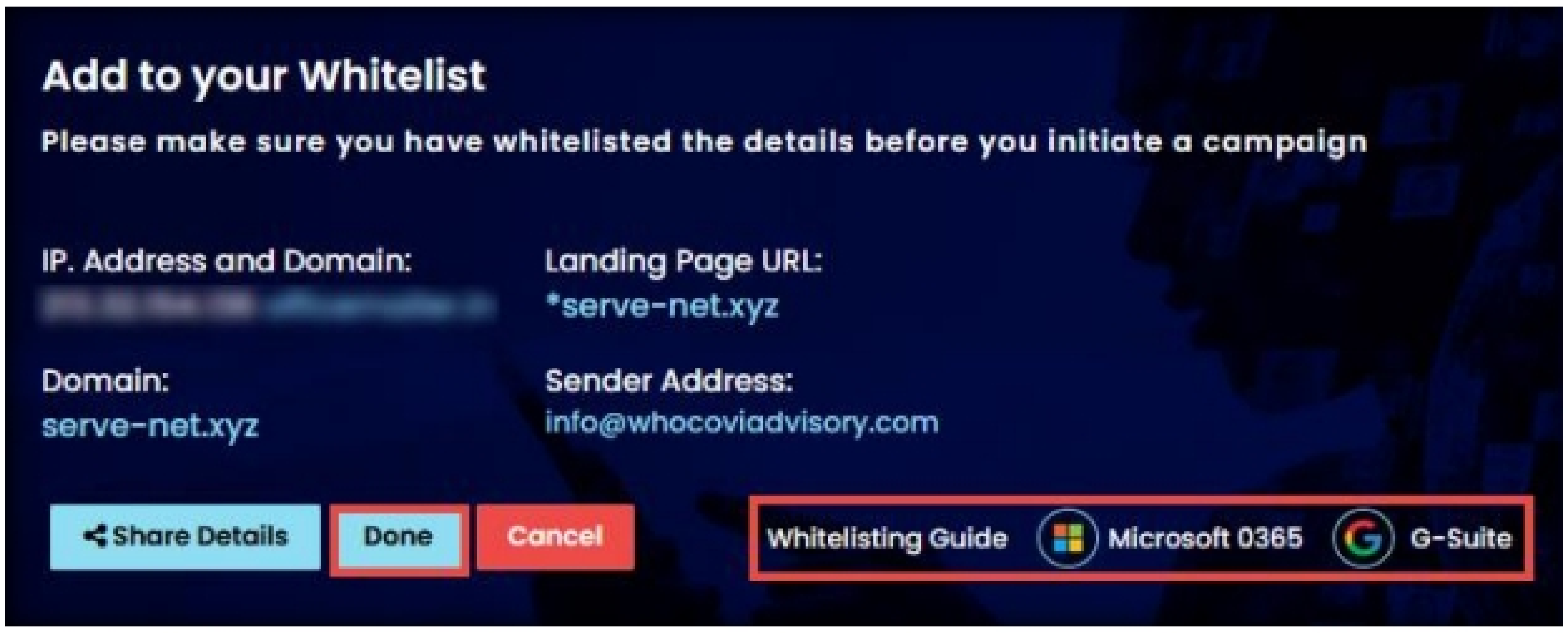
Dear {.Name},

Go through the attached document on safety measures regarding the spreading of corona virus or you can download the advisory from below button if you are having trouble while opening the attachment.

Figure 3.1.12: Create a phishing campaign

28. **Add to your Whitelist** pop-up appears, click **Done**.

Note: You must ensure that messages received from specific IP addresses do not get marked as spam. Do this by adding the addresses to an email whitelist in your Google Admin console. To do that, you can refer the whitelisting guide available for Microsoft O365 and G-Suite user accounts.



Add to your Whitelist

Please make sure you have whitelisted the details before you initiate a campaign

IP. Address and Domain: [redacted]

Landing Page URL: *serve-net.xyz

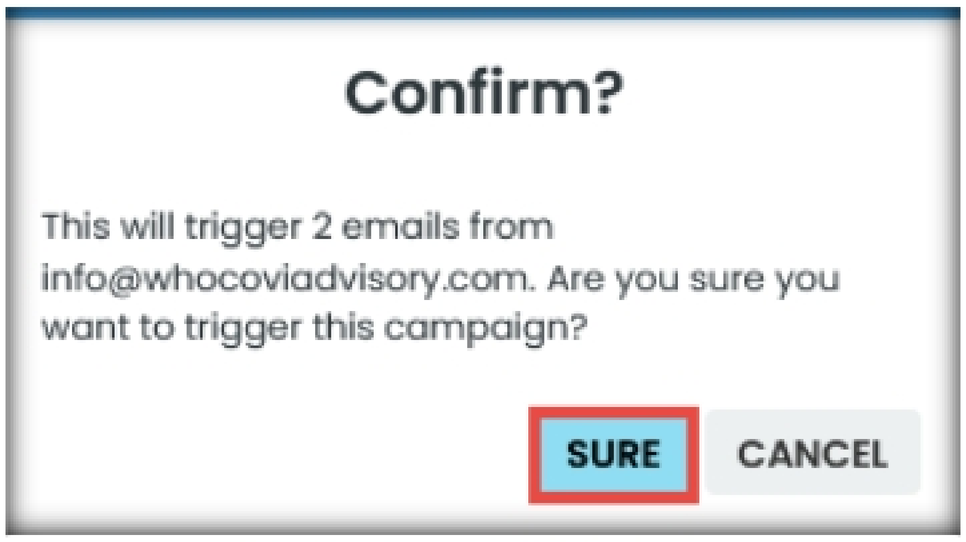
Domain: serve-net.xyz

Sender Address: info@whocoviadvisory.com

Share Details
Done
Cancel
Whitelisting Guide
Microsoft 0365
G-Suite

Figure 3.1.13: Add to your Whitelist pop-up

29. The **Confirm?** pop-up appears; click **SURE**.



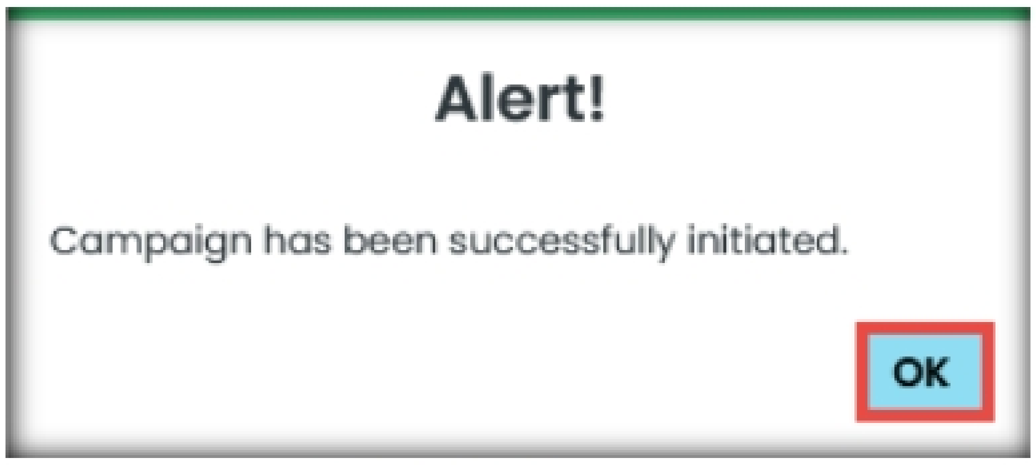
Confirm?

This will trigger 2 emails from info@whocoviadvisory.com. Are you sure you want to trigger this campaign?

Figure 3.1.14: Confirm pop-up

30. A count down timer appears and phishing campaign initiates in ten seconds.

31. The **Alert** pop-up appears, indicating successful initiation of a phishing campaign; click **OK**.



Alert!

Campaign has been successfully initiated.

Figure 3.1.15: Alert pop-up

32. Now, we must open the phishing email as a victim (here, an employee of the organization). To do so, turn on the **Windows Server 2019** virtual machine and login with the credentials **Administrator** and **Pa$$w0rd**.

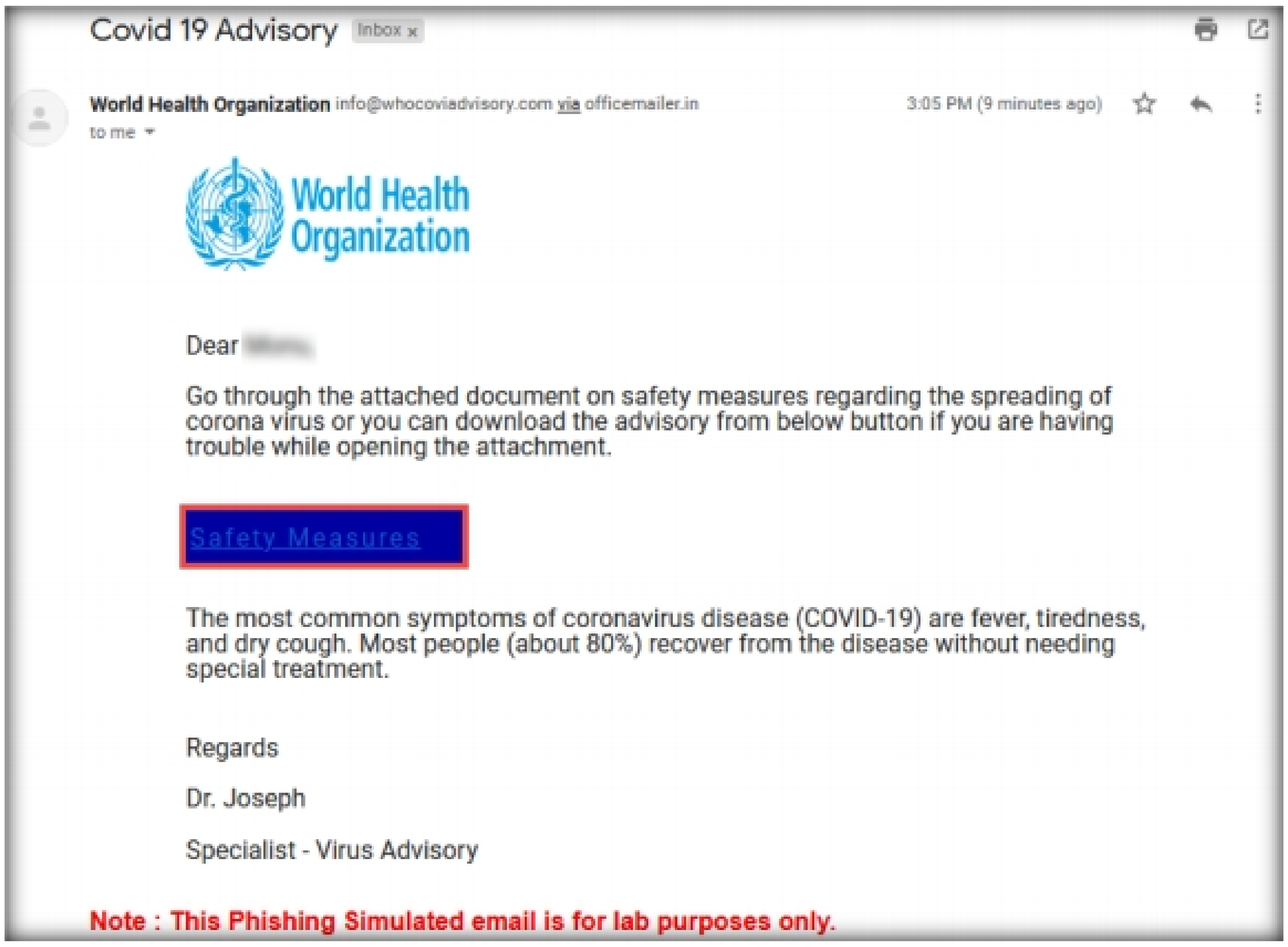
33. Open any web browser (here, **Mozilla Firefox**) and then open the email client provided while creating the phishing campaign (here, **Gmail**).

34. After you login to your **Gmail** account, search for an email with the subject **COVID 19 Advisory** in the **Inbox**.

Note: Depending on the security implementations of your organization, for example, if proper spam filters are enabled, this phishing email will end up in the **Spam** folder.

Note: If the email is not present in the **Inbox** folder, then check your **Spam** folder.

35. Click on the **Safety Measures** link in the email.


Covid 19 Advisory
Inbox x
World Health Organization info@whocoviadvisory.com via officemailer.in
to me
3:05 PM (9 minutes ago)
World Health Organization

Dear [redacted]

Go through the attached document on safety measures regarding the spreading of corona virus or you can download the advisory from below button if you are having trouble while opening the attachment.

Safety Measures

The most common symptoms of coronavirus disease (COVID-19) are fever, tiredness, and dry cough. Most people (about 80%) recover from the disease without needing special treatment.

Regards

Dr. Joseph

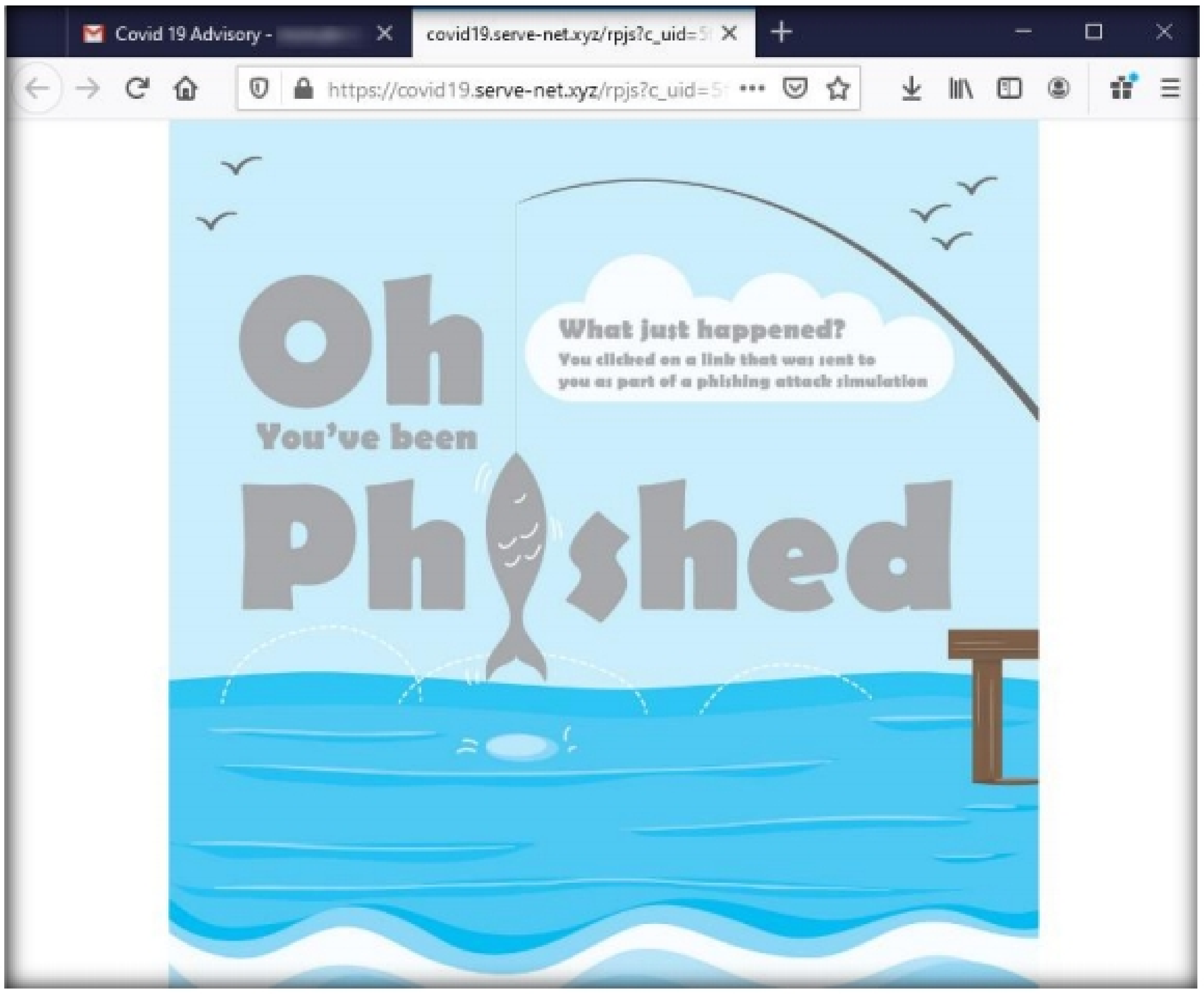
Specialist - Virus Advisory

Note : This Phishing Simulated email is for lab purposes only.

Figure 3.1.16: Phishing Email

36. If a **Suspicious link** pop-up appears, click **Proceed**.

37. The landing page **Oh You've been Phished** appears; as shown in the screenshot.


Covid 19 Advisory - [redacted]
covid19.serve-net.xyz/rpjs?c_uid=
https://covid19.serve-net.xyz/rpjs?c_uid=
Oh
You've been
Phished

What just happened?
You clicked on a link that was sent to you as part of a phishing attack simulation

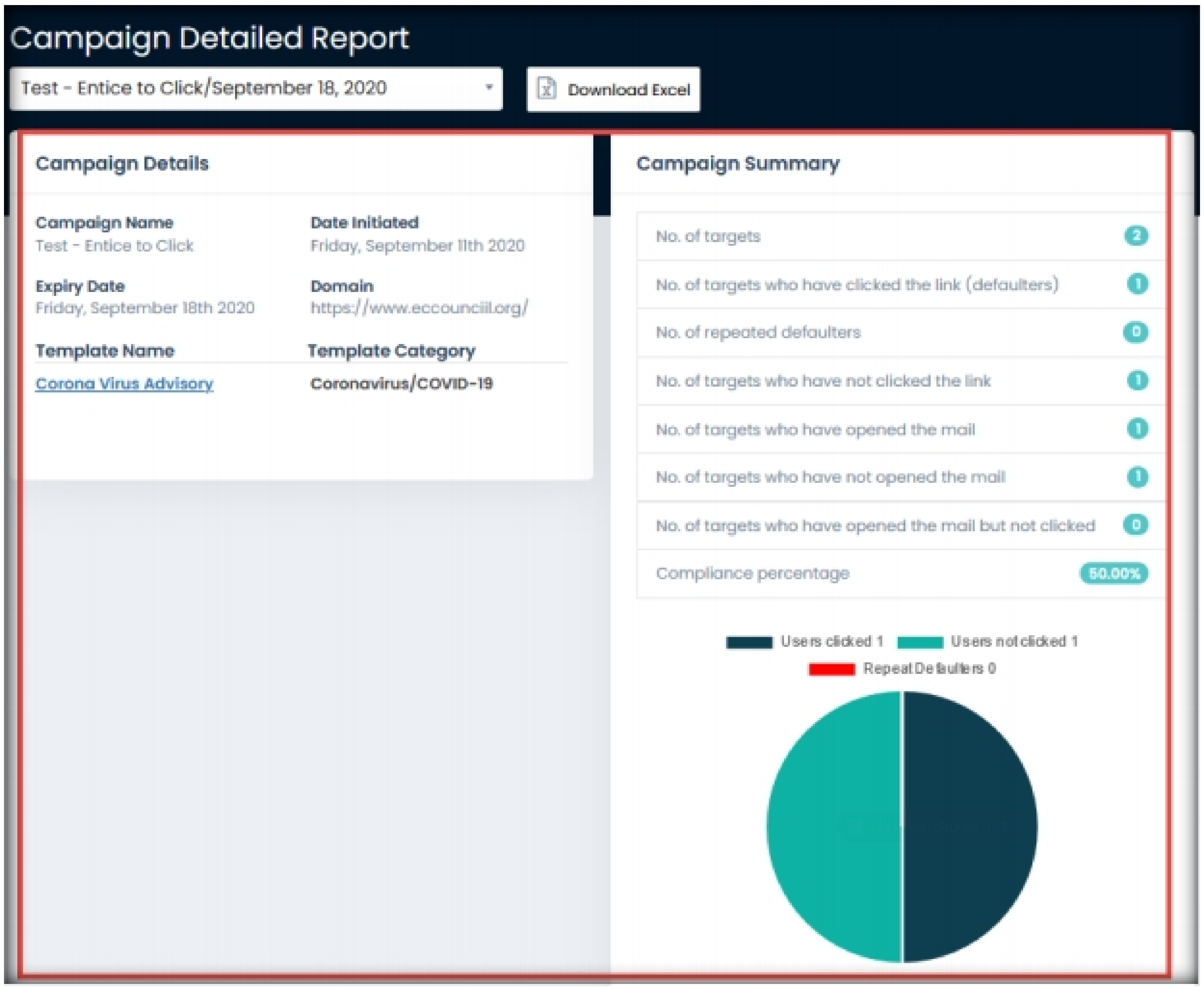
Figure 3.1.17: The landing page

38. Now, switch back to the **Windows 10** virtual machine.

39. Click on the **Test – Entice to Click** campaign present on the **OhPhish Dashboard**.

40. The **Campaign Detailed Report** page appears, displaying the **Campaign Details** and **Campaign Summary** sections.

41. In the **Campaign Summary** section, you can observe that the values of **No. of targets who have clicked the link (defaulters)** and **No. of Targets who have opened the mail** are both **1** (here, we have opened only one email account).


Campaign Detailed Report

Test - Entice to Click/September 18, 2020

Campaign Details

Campaign Name: Test - Entice to Click
Date Initiated: Friday, September 11th 2020
Expiry Date: Friday, September 18th 2020
Domain: https://www.eccounciil.org/
Template Name: Corona Virus Advisory
Template Category: Coronavirus/COVID-19

Campaign Summary

No. of targets	2
No. of targets who have clicked the link (defaulters)	1
No. of repeated defaulters	0
No. of targets who have not clicked the link	1
No. of targets who have opened the mail	1
No. of targets who have not opened the mail	1
No. of targets who have opened the mail but not clicked	0
Compliance percentage	50.00%

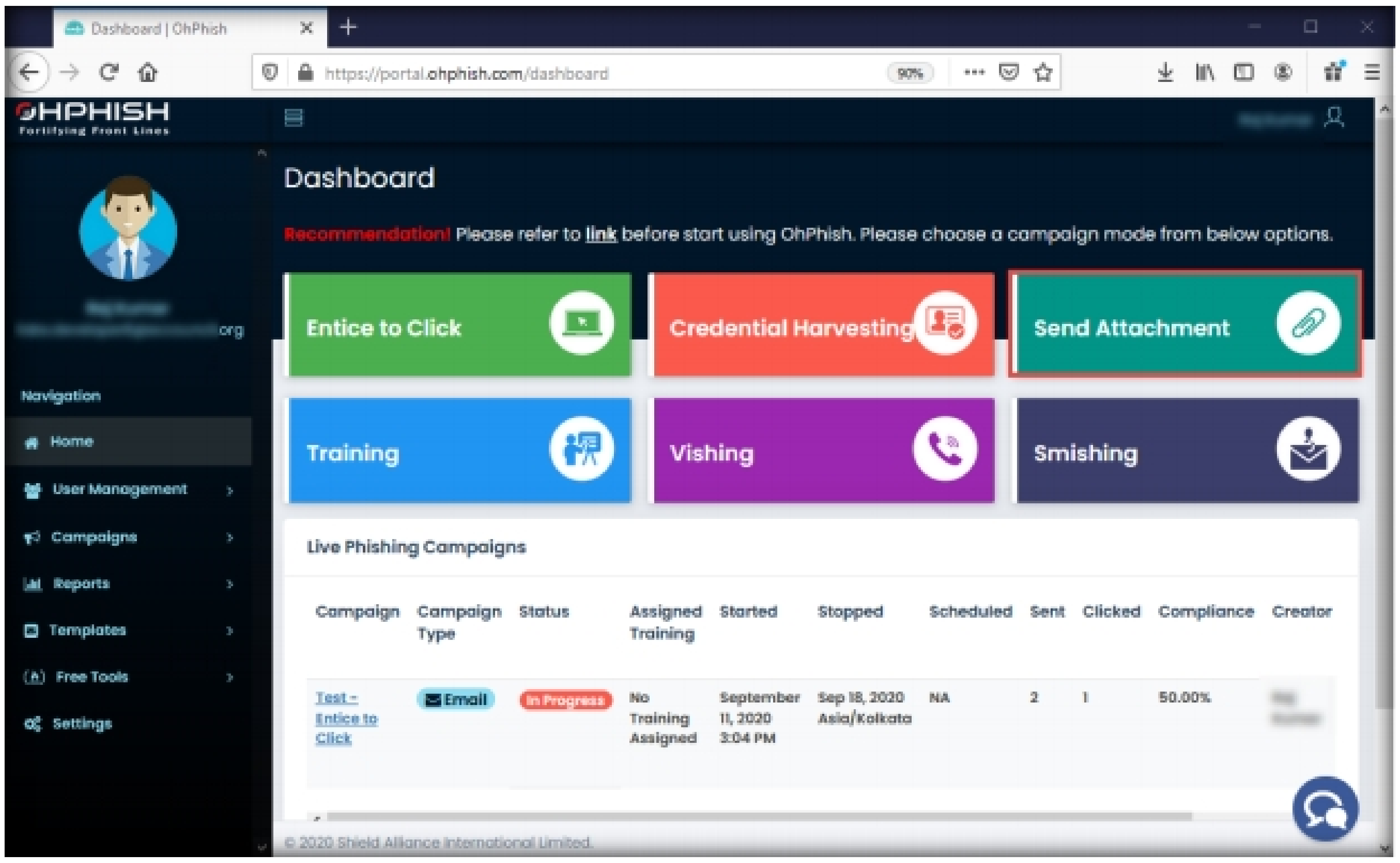
Figure 3.1.18: Campaign Detailed Report

TASK 1.3

Phish using Send Attachment

42. Now, click **Home** in the left pane to navigate back to the **OhPhish Dashboard**.

43. In the **OhPhish Dashboard**, click on the **Send Attachment** option.


Dashboard | OhPhish
https://portal.ohphish.com/dashboard
OHPHISH
Fortifying Front Lines
Navigation
Home
User Management
Campaigns
Reports
Templates
Free Tools
Settings
Entice to Click
Credential Harvesting
Send Attachment
Training
Vishing
Smishing

Dashboard

Recommendation! Please refer to link before start using OhPhish. Please choose a campaign mode from below options.

Live Phishing Campaigns

Campaign	Campaign Type	Status	Assigned Training	Started	Stopped	Scheduled	Sent	Clicked	Compliance	Creator
Test - Entice to Click	Email	In Progress	No Training Assigned	September 11, 2020 3:04 PM	Sep 18, 2020 Asia/Kolkata	NA	2	1	50.00%	[redacted]

© 2020 Shield Alliance International Limited.

Figure 3.1.19: OhPhish Dashboard

44. The **Create New Email Phishing Campaign** form appears.

45. In the **Campaign Name** field, enter any name (here, **Test – Send Attachment**). In the **Select Template Category** field, select **Office Mailers** from the drop-down list.

Note: Ensure that the **Existing templates** button is selected in the **Email Template** field.

46. In the **Select Country** field, leave the default option selected (**All**).

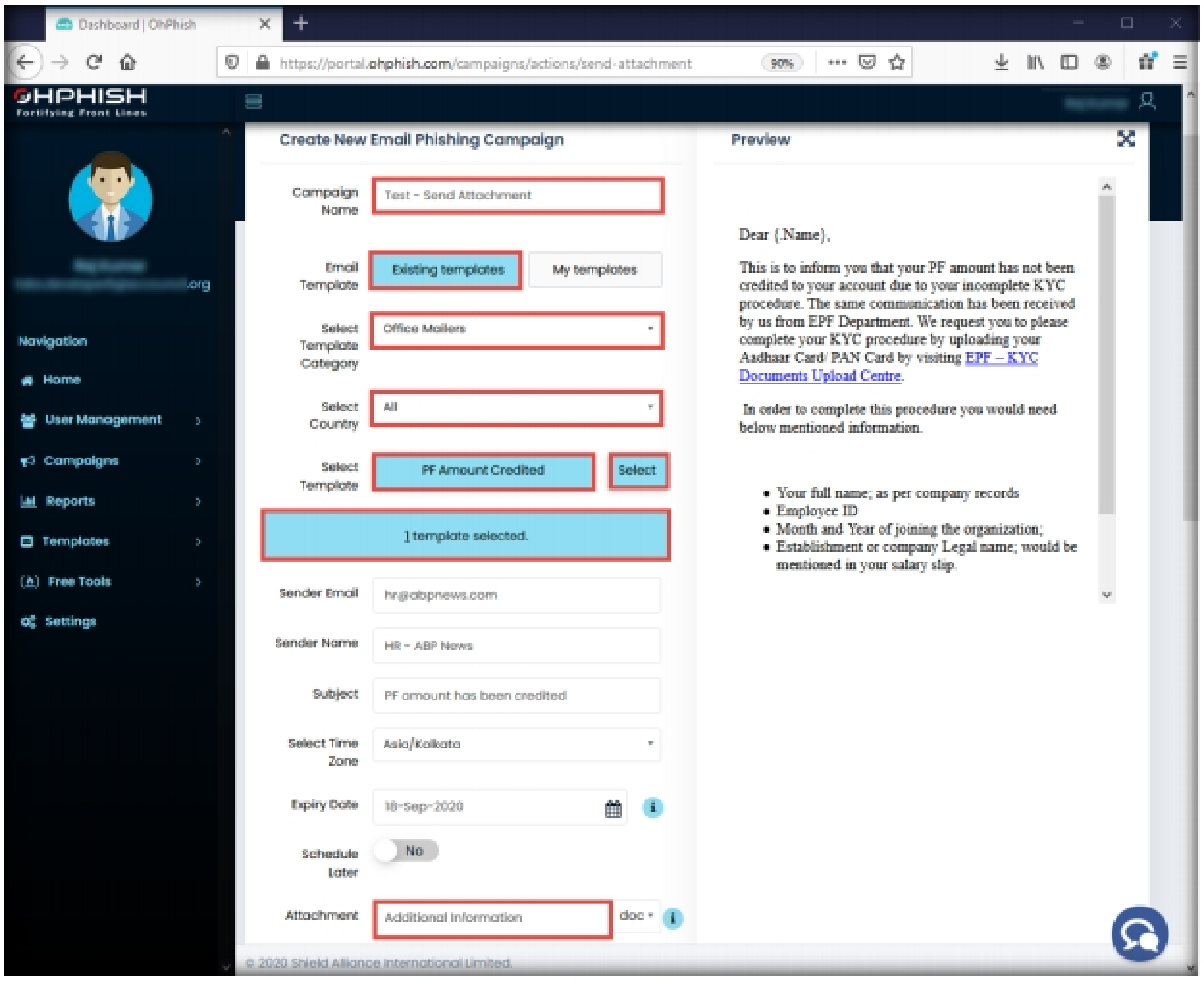
47. In the **Select Template** field, select the **PF Amount Credited** option from the drop-down list and then click the **Select** button.

48. Leave fields such as **Sender Email**, **Sender Name**, **Subject**, **Select Time Zone**, **Expiry Date**, and **Schedule Later** set to their default values, as shown in the screenshot.

Note: You can change the above-mentioned options if you want to.

49. In the **Attachment** field, enter any name (here, **Additional Information**).

Note: Ensure that the **Enable Macro** checkbox is not selected.


Dashboard | OhPhish
https://portal.ohphish.com/campaigns/actions/send-attachment
90%
OHPHISH
Fortifying Front Lines
[redacted]
[redacted].org
Navigation
Home
User Management
Campaigns
Reports
Templates
Free Tools
Settings
Existing templates
My templates
Select
© 2020 Shield Alliance International Limited.

Create New Email Phishing Campaign

Campaign Name: Test - Send Attachment

Email Template: Existing templates

Select Template Category: Office Mailers

Select Country: All

Select Template: PF Amount Credited

1 template selected.

Sender Email: hr@abpnews.com

Sender Name: HR - ABP News

Subject: PF amount has been credited

Select Time Zone: Asia/Kolkata

Expiry Date: 18-Sep-2020

Schedule Later: No

Attachment: Additional Information doc

Preview

Dear {.Name},

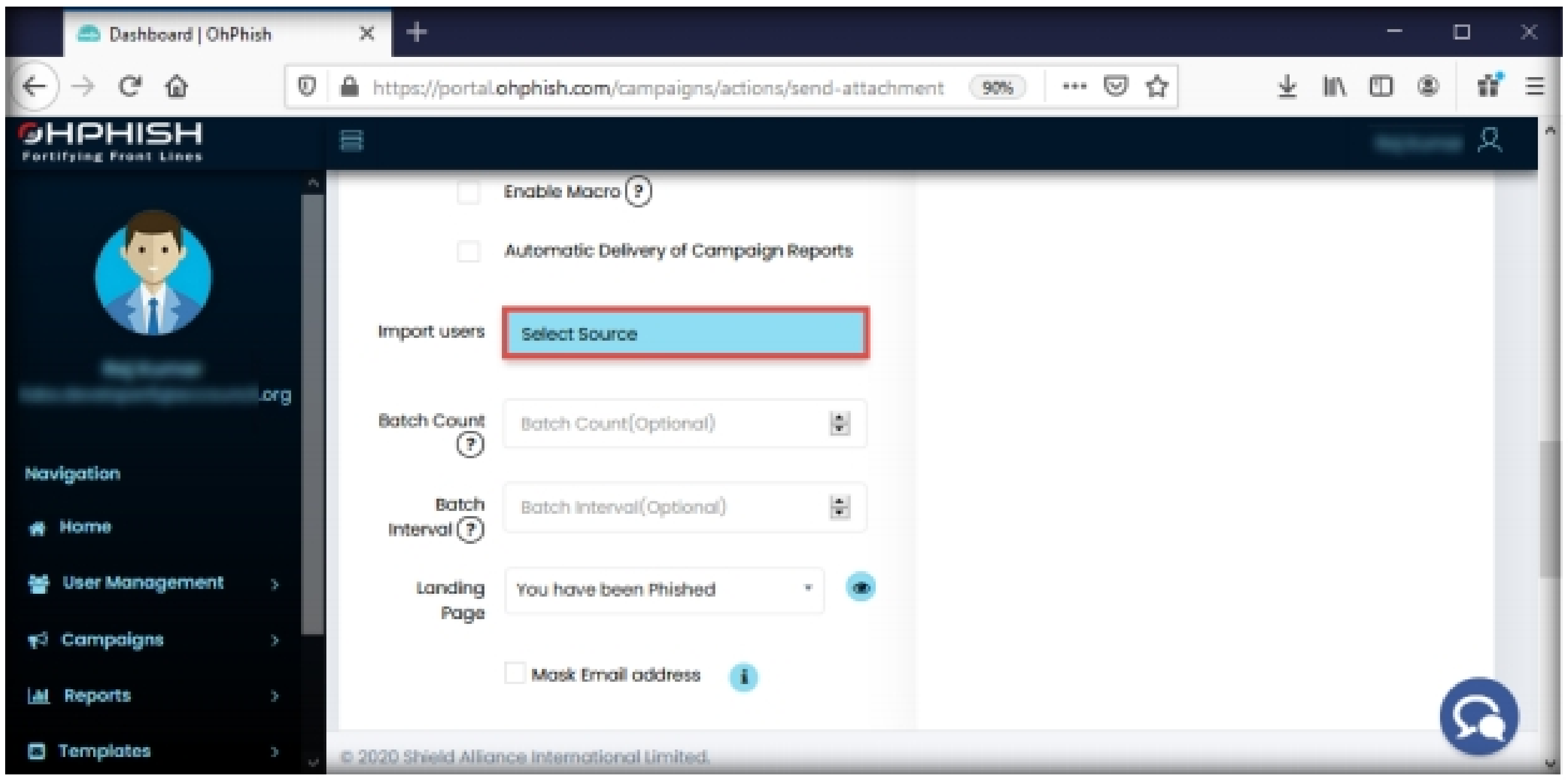
This is to inform you that your PF amount has not been credited to your account due to your incomplete KYC procedure. The same communication has been received by us from EPF Department. We request you to please complete your KYC procedure by uploading your Aadhaar Card/ PAN Card by visiting EPF – KYC Documents Upload Centre.

In order to complete this procedure you would need below mentioned information.

- Your full name; as per company records
- Employee ID
- Month and Year of joining the organization;
- Establishment or company Legal name; would be mentioned in your salary slip.

Figure 3.1.20: Create New Email Phishing Campaign

50. Click **Select Source** button under **Import users** field.


Dashboard | OhPhish
https://portal.ohphish.com/campaigns/actions/send-attachment
90%
OHPHISH
Fortifying Front Lines
[redacted]
[redacted].org
Navigation
Home
User Management
Campaigns
Reports
Templates
Select Source
© 2020 Shield Alliance International Limited.

☐ Enable Macro (?)

☐ Automatic Delivery of Campaign Reports

Import users: Select Source

Batch Count (?): Batch Count(Optional)

Batch Interval (?): Batch Interval(Optional)

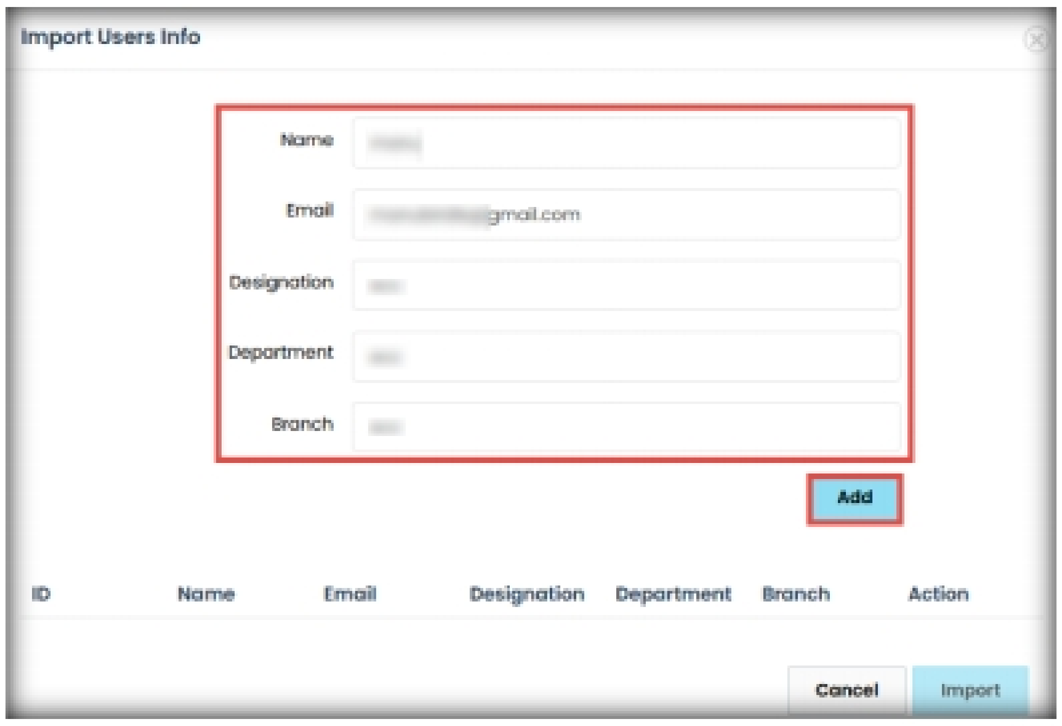
Landing Page: You have been Phished

☐ Mask Email address

Figure 3.1.21: Create New Email Phishing Campaign form

51. **Import Users** pop-up appears, click to select the **Quick Add** option from the list of options

52. The **Import Users Info** pop-up appears; enter the details of the employee and click **Add**.


Import Users Info
Add
ID
Name
Email
Designation
Department
Branch
Action
Cancel
Import

Name: [redacted]

Email: [redacted]gmail.com

Designation: [redacted]

Department: [redacted]

Branch: [redacted]

Figure 3.1.22: Import Users Info

53. Similarly, you can add the details of multiple users. Here, we added three users.

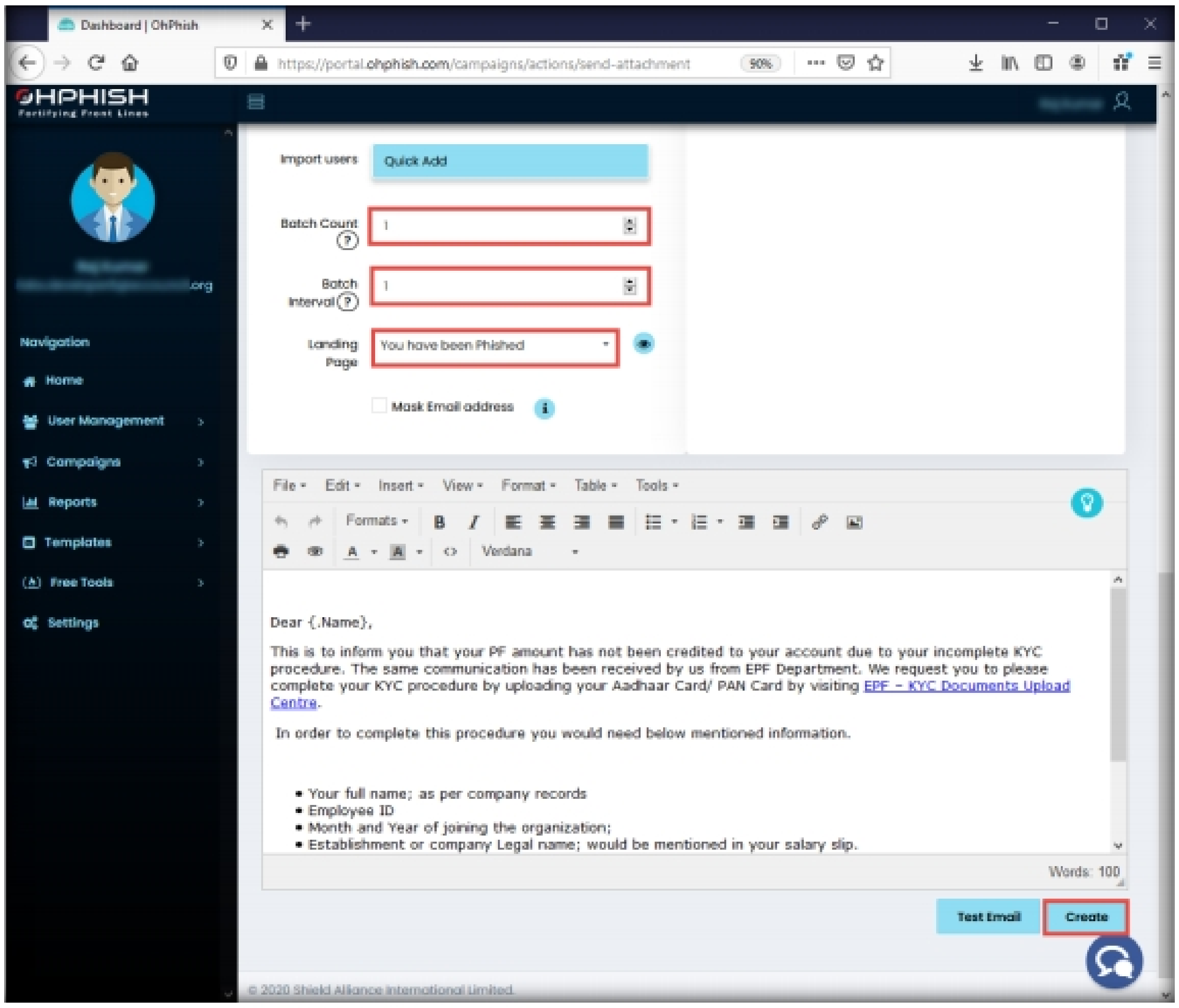
54. After adding the users' details, click **Import**.

55. In the **Batch Count** and **Batch Interval** fields, set the values to **1**.

Note: The values of Batch Count and Batch Interval might differ depending on the number of users you are sending phishing emails to.

56. Leave the **Landing Page** field set to its default value.

57. Scroll down to the end of the page and click **Create** to create the phishing campaign.


Dashboard | OhPhish
https://portal.ohphish.com/campaigns/actions/send-attachment
90%
OHPHISH
Fortifying Front Lines
Navigation
Home
User Management
Campaigns
Reports
Templates
Free Tools
Settings
Import users
Quick Add
File
Edit
Insert
View
Format
Table
Tools
Formats
Verdana
Words: 100
Test Email
Create
© 2020 Shield Alliance International Limited.

[redacted]

[redacted].org

Batch Count: 1

Batch Interval: 1

Landing Page: You have been Phished

☐ Mask Email address

Dear {.Name},

This is to inform you that your PF amount has not been credited to your account due to your incomplete KYC procedure. The same communication has been received by us from EPF Department. We request you to please complete your KYC procedure by uploading your Aadhaar Card/ PAN Card by visiting EPF – KYC Documents Upload Centre.

In order to complete this procedure you would need below mentioned information.

- Your full name; as per company records
- Employee ID
- Month and Year of joining the organization;
- Establishment or company Legal name; would be mentioned in your salary slip.

Figure 3.1.23: Click Create to create a phishing campaign

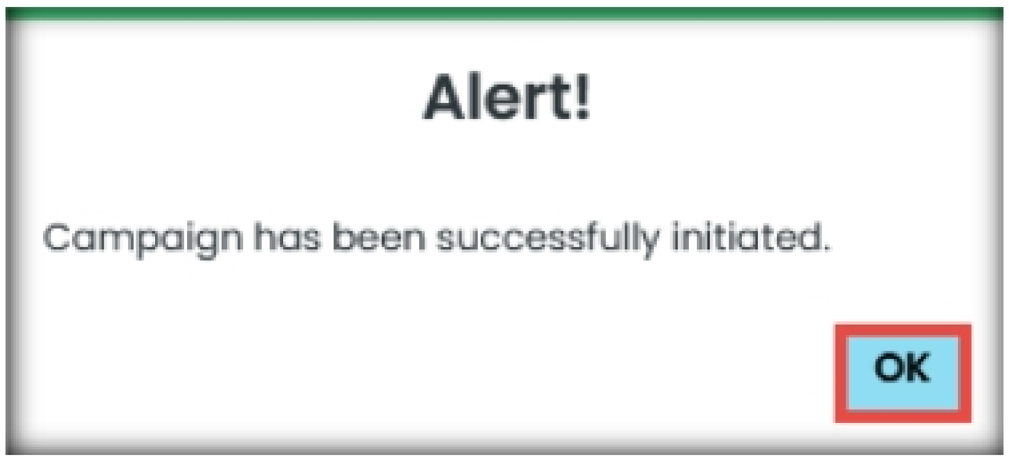
58. **Add to your Whitelist** pop-up appears, click **Done**.

Note: You must ensure that messages received from specific IP addresses do not get marked as spam. Do this by adding the addresses to an email whitelist in your Google Admin console. To do that, you can refer the whitelisting guide available for Microsoft O365 and G-Suite user accounts.

59. The **Confirm?** pop-up appears; click **SURE**.

60. A count down timer appears and phishing campaign initiates in ten seconds.

61. The **Alert!** pop-up appears, indicating successful initiation of a phishing campaign; click **OK**.



Alert!

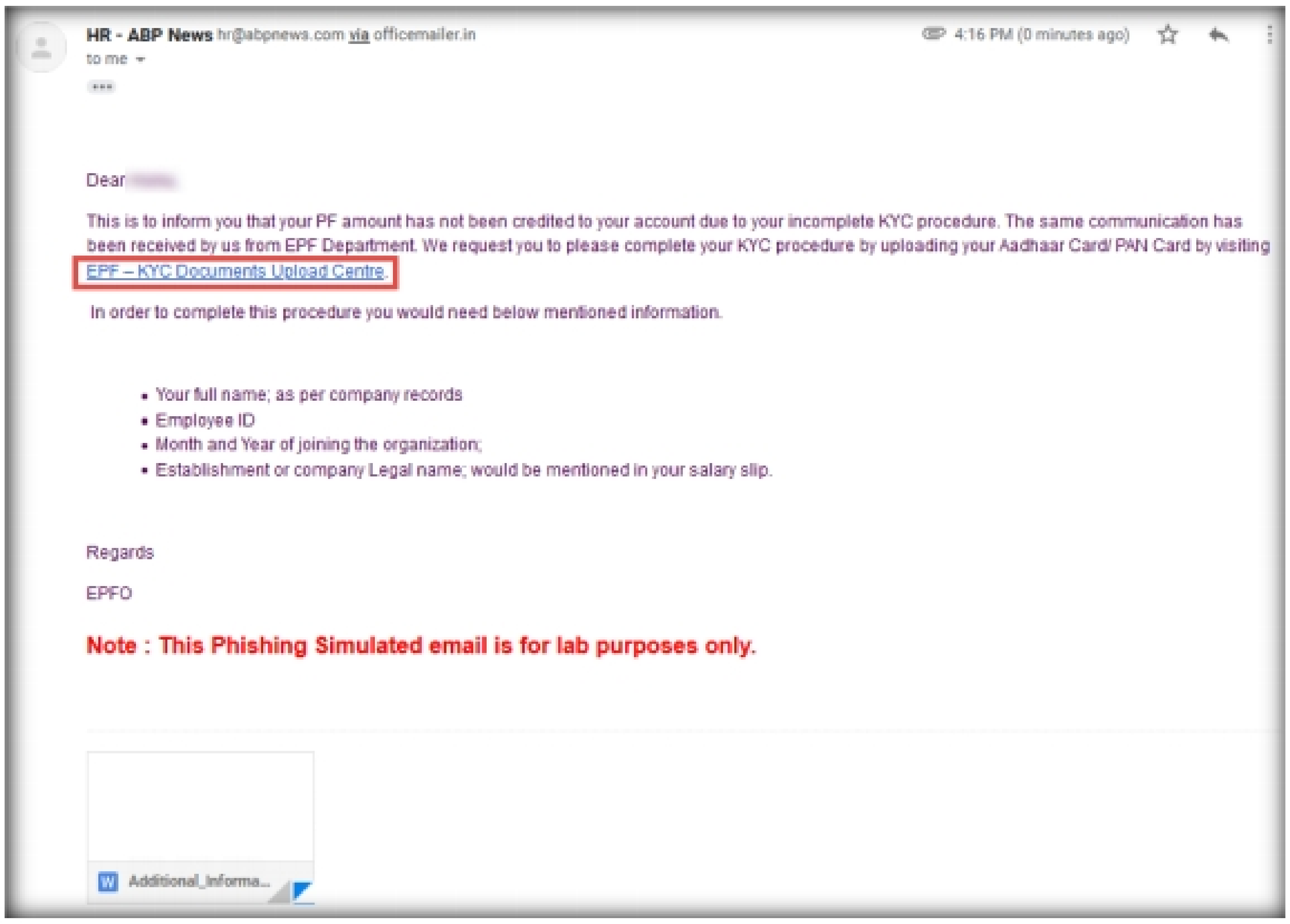
Campaign has been successfully initiated.

Figure 3.1.24: Alert pop-up

62. Now, switch to the **Windows Server 2019** virtual machine and open the **Inbox** of the **Gmail** account opened previously.

63. You will find an email from **HR – ABP News**, as shown in the screenshot.

64. Click on the **EPF – KYC Documents Upload Centre** hyperlink present in the email.



HR - ABP News hr@abpnews.com via officemailer.in
to me

Dear [redacted]

This is to inform you that your PF amount has not been credited to your account due to your incomplete KYC procedure. The same communication has been received by us from EPF Department. We request you to please complete your KYC procedure by uploading your Aadhaar Card/ PAN Card by visiting EPF – KYC Documents Upload Centre.

In order to complete this procedure you would need below mentioned information.

- Your full name; as per company records
- Employee ID
- Month and Year of joining the organization;
- Establishment or company Legal name; would be mentioned in your salary slip.

Regards

EPFO

Note : This Phishing Simulated email is for lab purposes only.

Figure 3.1.25: Phishing email

65. If a **Suspicious link** pop-up appears, click **Proceed**.

66. You will be re-directed to the **Oh You've been Phished** landing page, as shown in the screenshot.

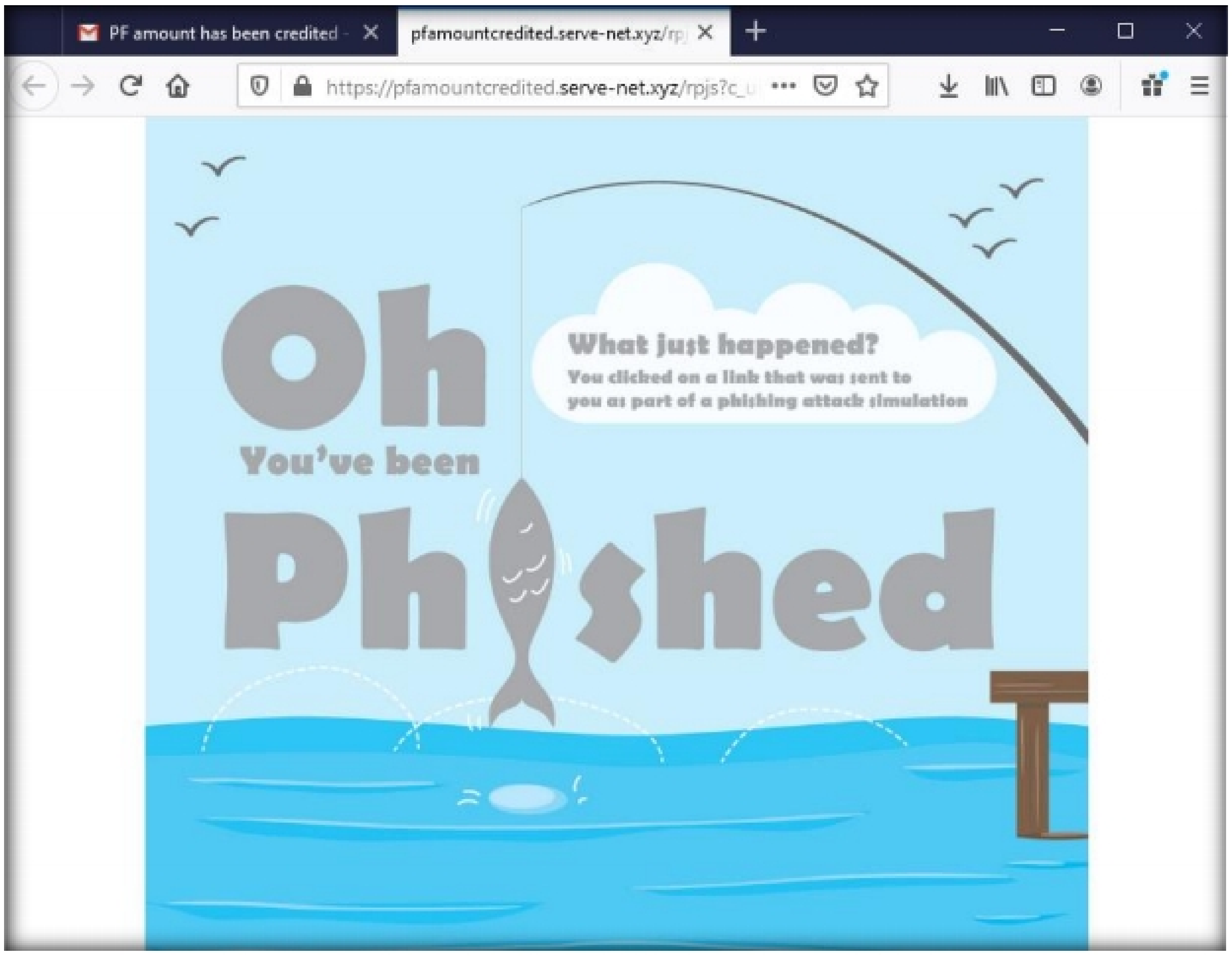

PF amount has been credited
pfamountcredited.serve-net.xyz/rp
https://pfamountcredited.serve-net.xyz/rpjs?c_u
Oh
You've been
Phished
What just happened?
You clicked on a link that was sent to you as part of a phishing attack simulation

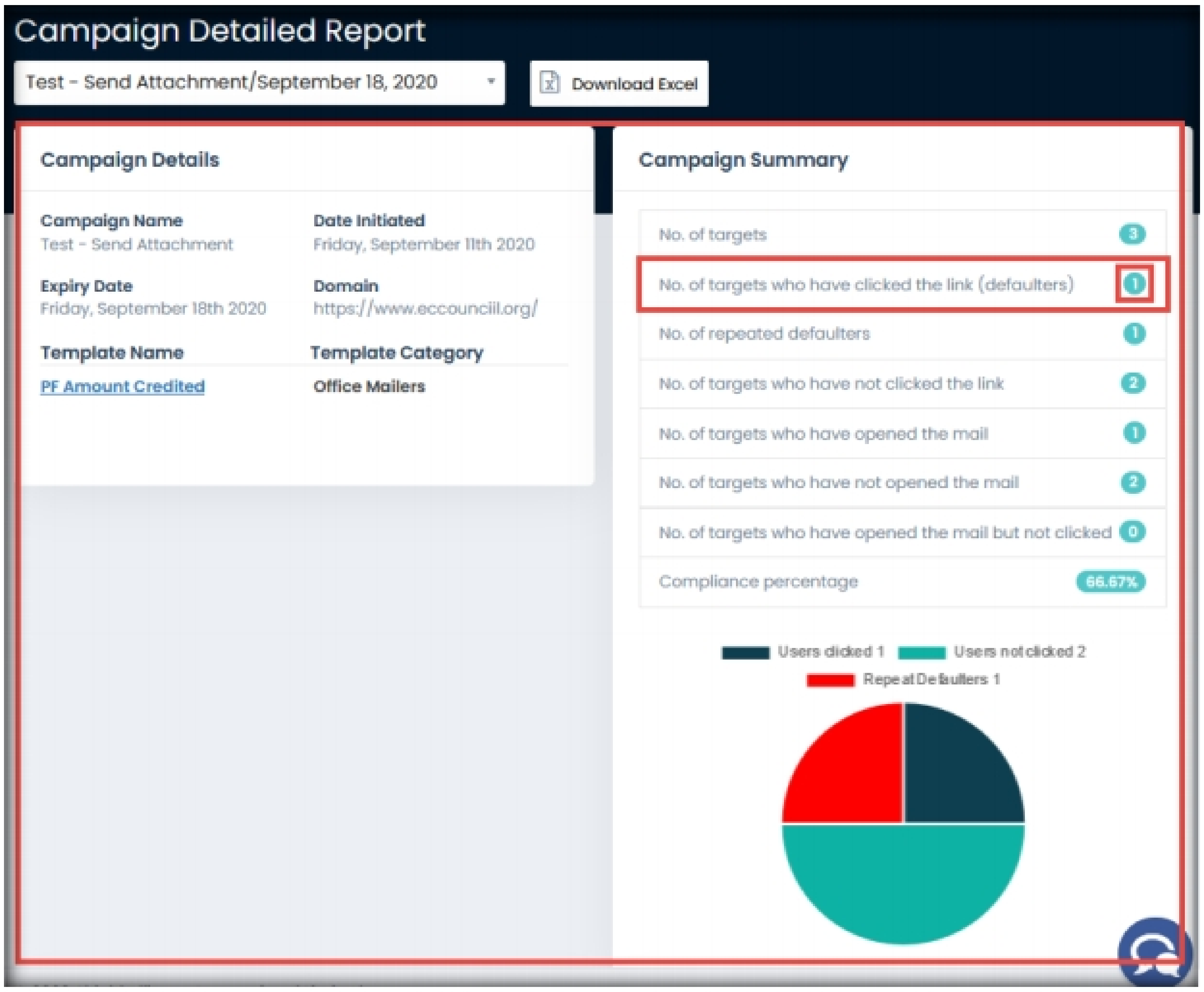
Figure 3.1.26: Phishing email

67. Now, switch back to the **Windows 10** virtual machine.

68. Click on the **Test – Send Attachment** campaign present on the **OhPhish Dashboard**.

69. The **Campaign Detailed Report** page appears, displaying the **Campaign Details** and **Campaign Summary** sections.

70. In the **Campaign Summary** section, you can observe that the value of **No. of targets who have clicked the link (defaulters)** is **1**. Click on ❶ to see the defaulter.



Campaign Detailed Report

Test - Send Attachment/September 18, 2020

Campaign Details

Campaign Name
Test - Send Attachment

Date Initiated
Friday, September 11th 2020

Expiry Date
Friday, September 18th 2020

Domain
https://www.eccouncil.org/

Template Name
PF Amount Credited

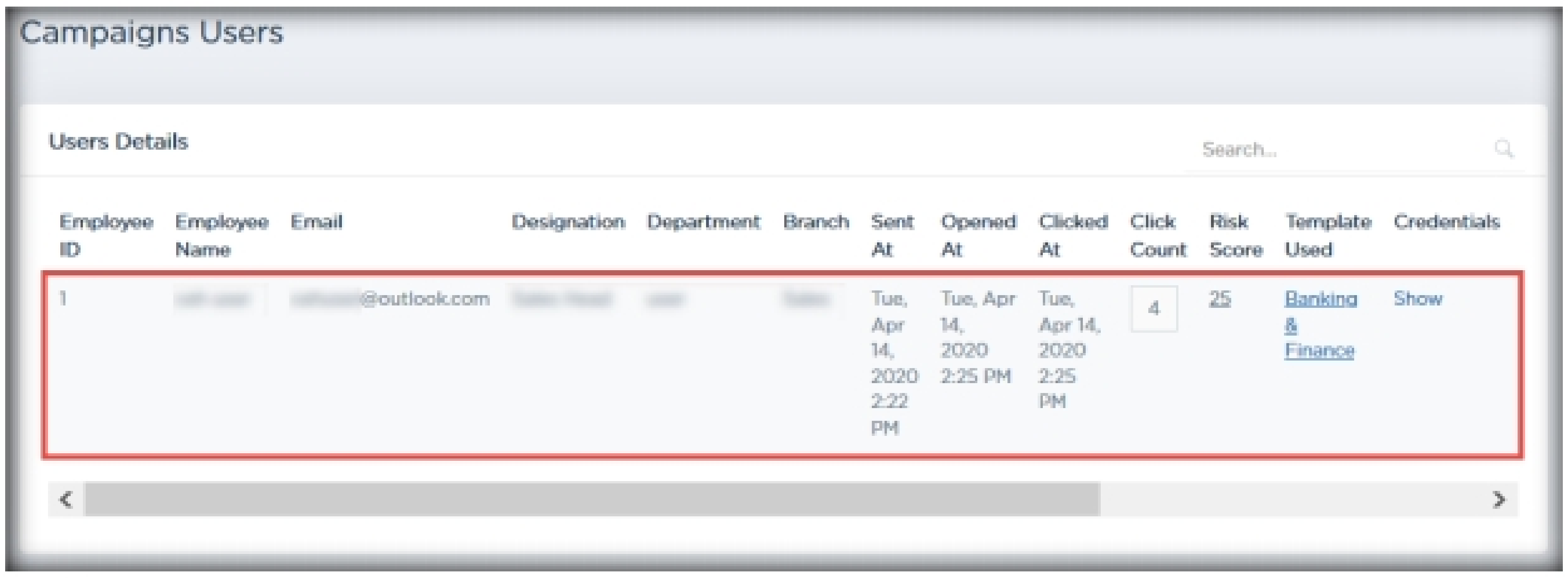
Template Category
Office Mailers

Campaign Summary

No. of targets	3
No. of targets who have clicked the link (defaulters)	1
No. of repeated defaulters	1
No. of targets who have not clicked the link	2
No. of targets who have opened the mail	1
No. of targets who have not opened the mail	2
No. of targets who have opened the mail but not clicked	0
Compliance percentage	66.67%

Figure 3.1.27: Campaign Detailed Report

71. The **Campaigns Users** page appears, displaying the details of the defaulter, such as **Risk Score**, **Credentials**, **IP Address**, **Location**, etc., as shown in the screenshot.



Campaigns Users

Users Details

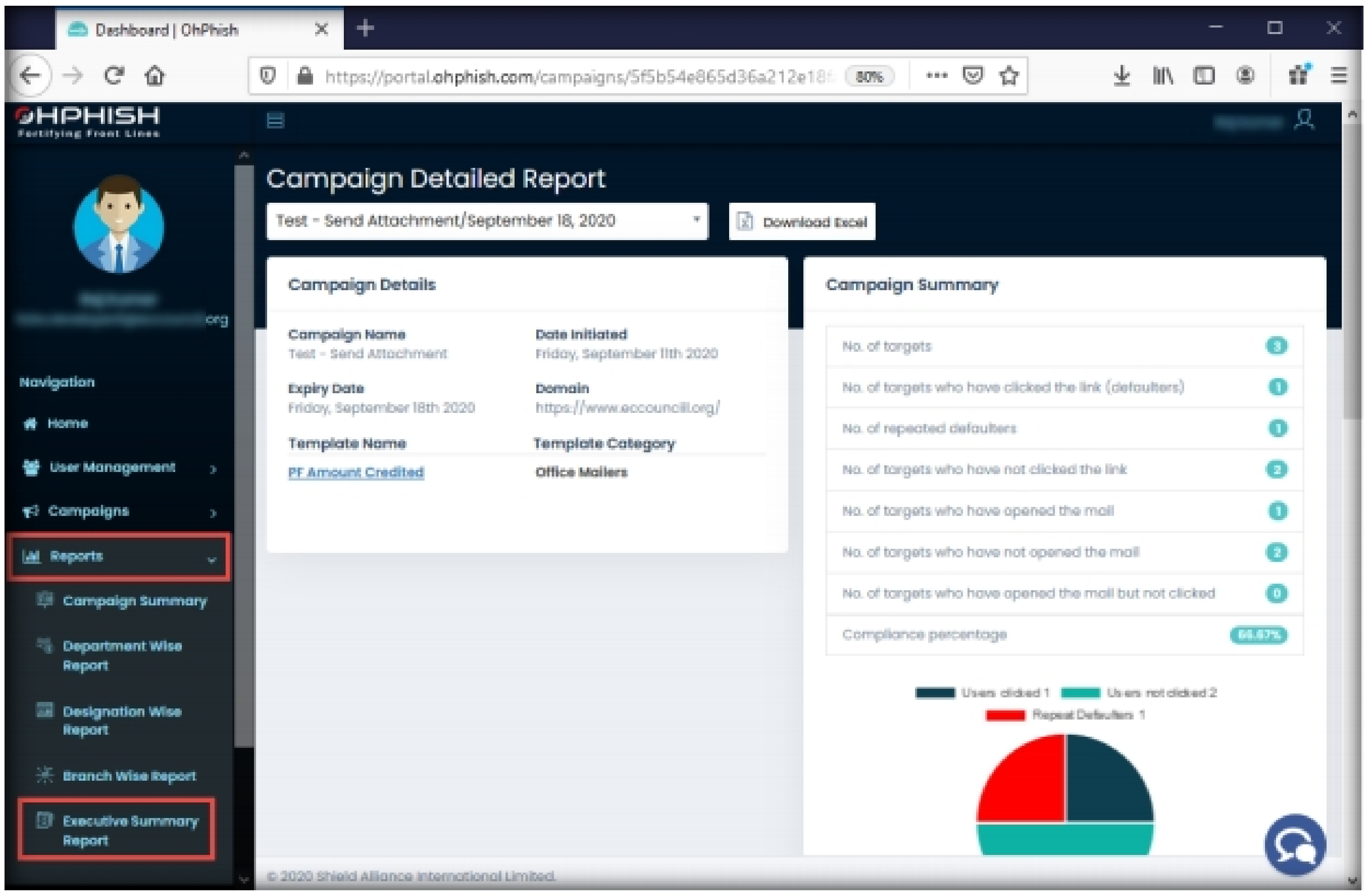
Employee ID	Employee Name	Email	Designation	Department	Branch	Sent At	Opened At	Clicked At	Click Count	Risk Score	Template Used	Credentials
1	[redacted]	[redacted]@outlook.com	[redacted]	[redacted]	[redacted]	Tue, Apr 14, 2020 2:22 PM	Tue, Apr 14, 2020 2:25 PM	Tue, Apr 14, 2020 2:25 PM	4	25	Banking & Finance	Show

Figure 3.1.28: Campaign Users

TASK 1.4

Generate Phishing Report

72. Now, click to expand the **Reports** section in the left pane and select the **Executive Summary Report** option.


Dashboard | OhPhish
https://portal.ohphish.com/campaigns/5f5b54e865d36a212e18
80%
OHPHISH
Fortifying Front Lines
Navigation
Home
User Management
Campaigns
Reports
Campaign Summary
Department Wise Report
Designation Wise Report
Branch Wise Report
Executive Summary Report
Download Excel
Users clicked 1
Users not clicked 2
Repeat Defaulters 1

Campaign Detailed Report

Test - Send Attachment/September 18, 2020

Campaign Details

Campaign Name: Test - Send Attachment
Date Initiated: Friday, September 11th 2020
Expiry Date: Friday, September 18th 2020
Domain: https://www.eccouncil.org/
Template Name: PF Amount Credited
Template Category: Office Mailers

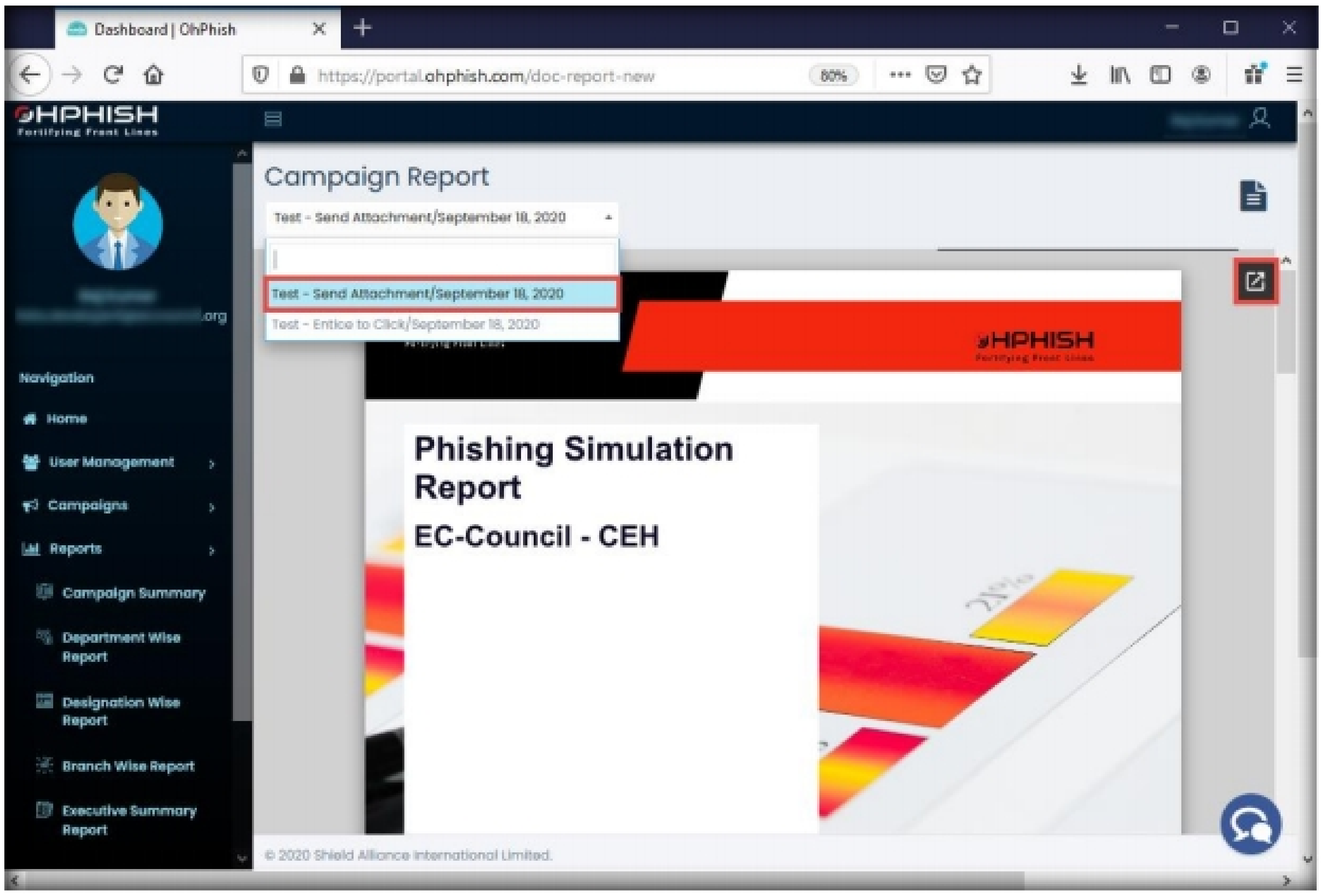
Campaign Summary

No. of targets	3
No. of targets who have clicked the link (defaulters)	1
No. of repeated defaulters	1
No. of targets who have not clicked the link	2
No. of targets who have opened the mail	1
No. of targets who have not opened the mail	2
No. of targets who have opened the mail but not clicked	0
Compliance percentage	66.67%

© 2020 Shield Alliance International Limited.

Figure 3.1.29: Generating Reports

73. The **Campaign Report** page appears; select any phishing campaign from the drop-down list (here, **Test – Send Attachment**) and click on the **Export** icon (📄) to export the report.


Dashboard | OhPhish
https://portal.ohphish.com/doc-report-new
80%
OHPHISH
Fortifying Front Lines
Navigation
Home
User Management
Campaigns
Reports
Campaign Summary
Department Wise Report
Designation Wise Report
Branch Wise Report
Executive Summary Report
OHPHISH
Fortifying Front Lines

Campaign Report

Test - Send Attachment/September 18, 2020

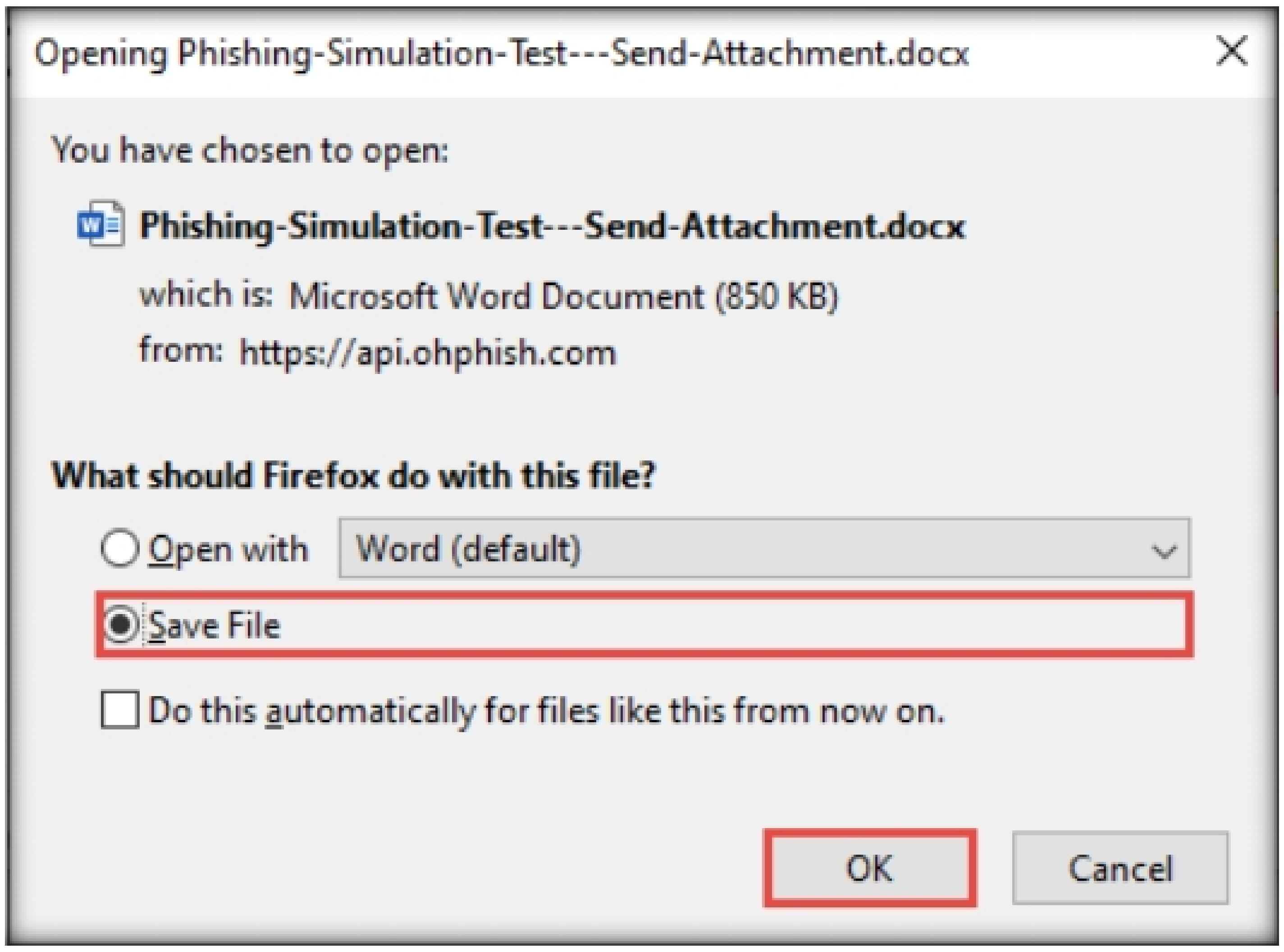
Test - Send Attachment/September 18, 2020
Test - Entice to Click/September 18, 2020

Phishing Simulation Report
EC-Council - CEH

© 2020 Shield Alliance International Limited.

Figure 3.1.30: Campaign Report

74. The **Opening Phishing-Simulation-Test** window appears; select the **Save File** radio button and click **OK**.



Opening Phishing-Simulation-Test---Send-Attachment.docx

You have chosen to open:

Phishing-Simulation-Test---Send-Attachment.docx

which is: Microsoft Word Document (850 KB)
from: https://api.ohphish.com

What should Firefox do with this file?

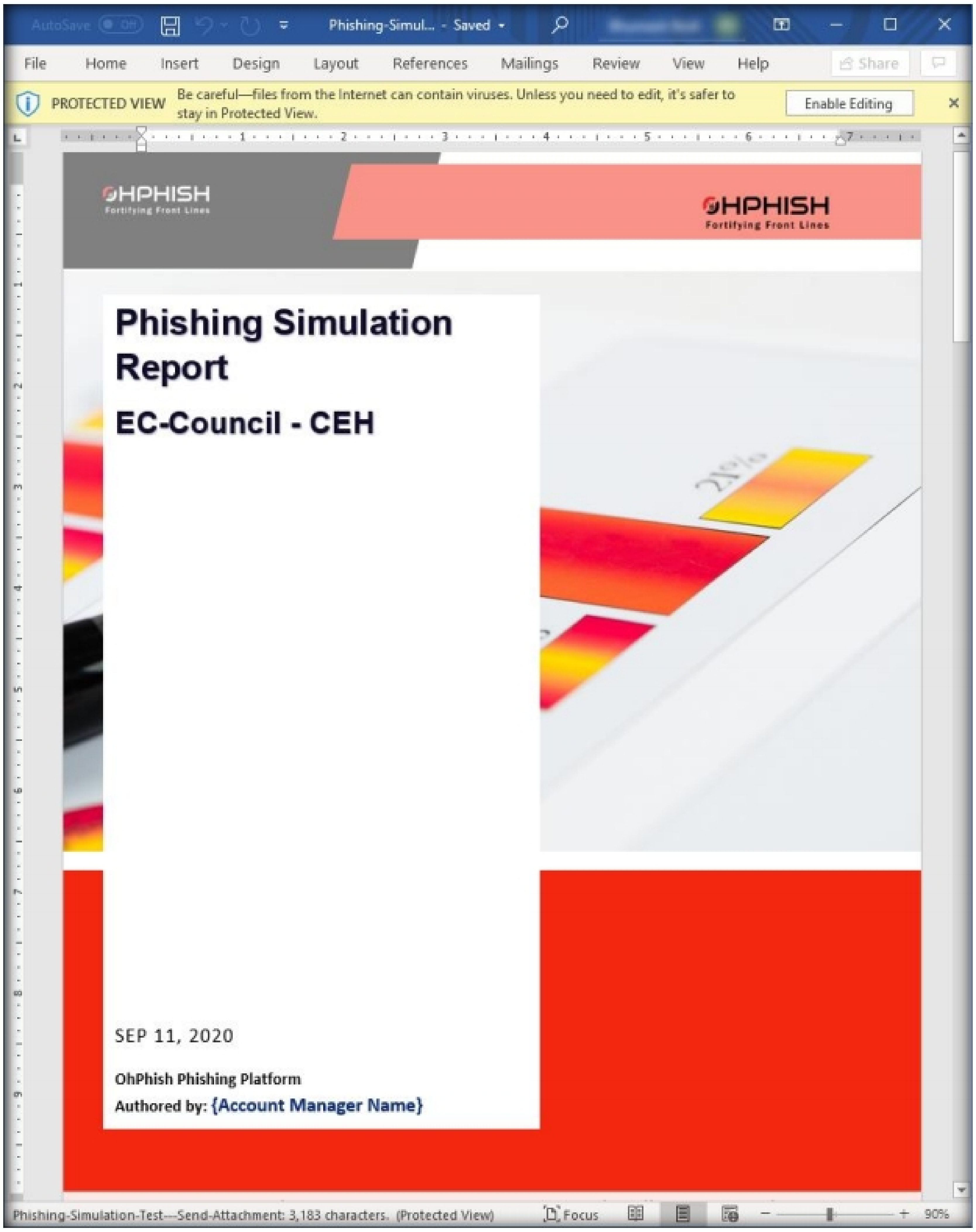
○ Open with Word (default)
● Save File
☐ Do this automatically for files like this from now on.

Figure 3.1.31: Opening Phishing-Simulation-Test window

75. The file is downloaded to the default location (here, **Downloads**). Navigate to the download location and double-click the **Phishing-Simulation-Test---Send-Attachment** file to open it.

76. The executive phishing report appears in the document, as shown in the screenshot.

Note: You can also explore other report options such as **Department Wise Report**, **Designation Wise Report**, and **Branch Wise Report**.



Phishing-Simul... - Saved
File
Home
Insert
Design
Layout
References
Mailings
Review
View
Help
Share
PROTECTED VIEW
Enable Editing
OHPHISH
Fortifying Front Lines
Focus
90%

Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

Phishing Simulation Report

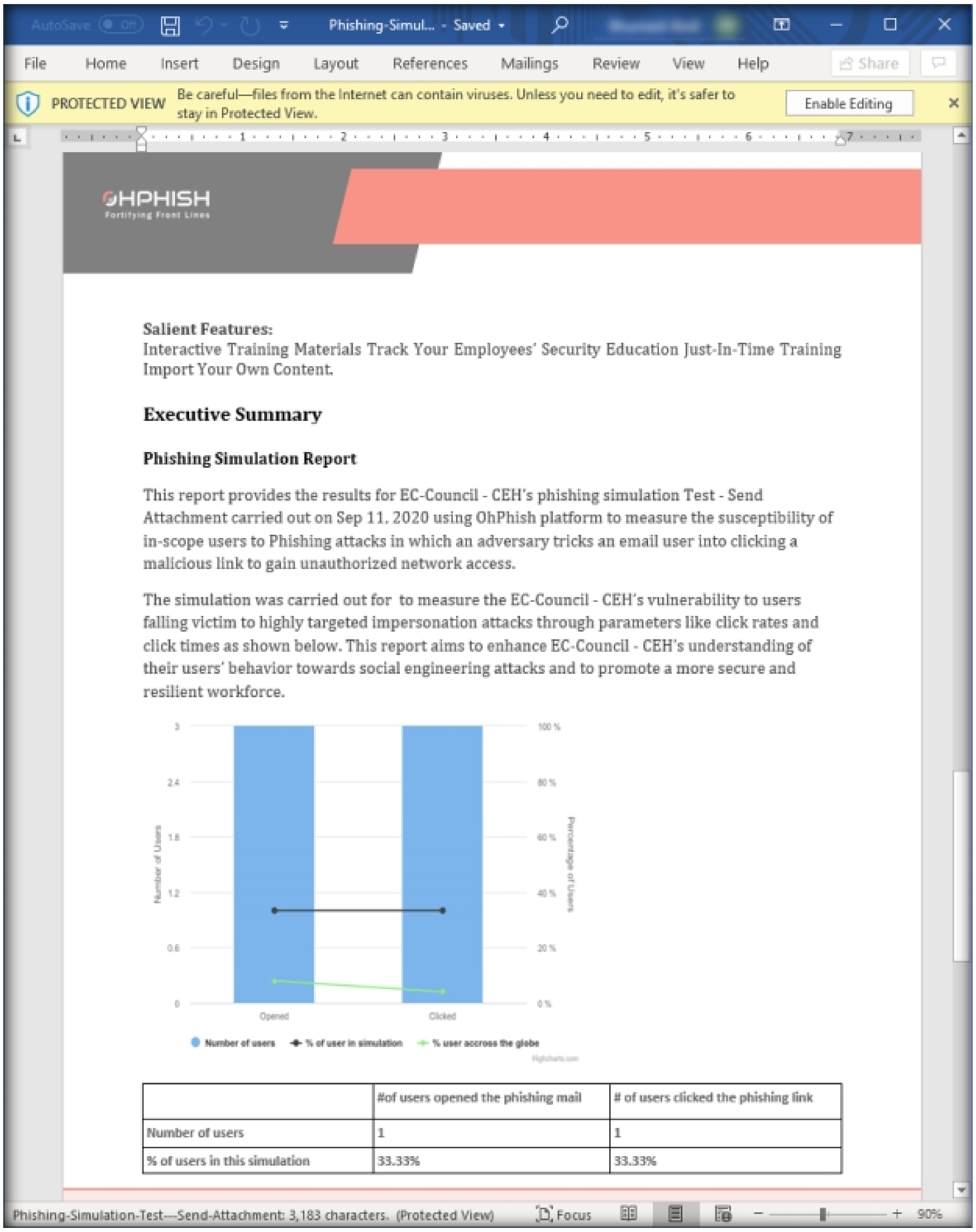
EC-Council - CEH

SEP 11, 2020

OhPhish Phishing Platform
Authored by: {Account Manager Name}

Phishing-Simulation-Test---Send-Attachment: 3,183 characters. (Protected View)

Figure 3.1.32: Campaign Report page


AutoSave Off
Phishing-Simul... - Saved
[redacted]
File
Home
Insert
Design
Layout
References
Mailings
Review
View
Help
Share
PROTECTED VIEW
Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.
Enable Editing
OHPHISH
Fortifying Front Lines

Salient Features:
Interactive Training Materials Track Your Employees' Security Education Just-In-Time Training Import Your Own Content.

Executive Summary

Phishing Simulation Report

This report provides the results for EC-Council - CEH's phishing simulation Test - Send Attachment carried out on Sep 11, 2020 using OhPhish platform to measure the susceptibility of in-scope users to Phishing attacks in which an adversary tricks an email user into clicking a malicious link to gain unauthorized network access.

The simulation was carried out for to measure the EC-Council - CEH's vulnerability to users falling victim to highly targeted impersonation attacks through parameters like click rates and click times as shown below. This report aims to enhance EC-Council - CEH's understanding of their users' behavior towards social engineering attacks and to promote a more secure and resilient workforce.

3
2.4
1.8
1.2
0.6
0
Number of Users
100 %
80 %
60 %
40 %
20 %
0 %
Percentage of Users
Opened
Clicked
● Number of users
◆ % of user in simulation
+ % user accross the globe
Highcharts.com

	#of users opened the phishing mail	# of users clicked the phishing link
Number of users	1	1
% of users in this simulation	33.33%	33.33%

Phishing-Simulation-Test---Send-Attachment: 3,183 characters. (Protected View)
Focus
90%

Figure 3.1.33: Campaign Report page

77. If you have an upgraded OhPhish account you can also explore other phishing methods such as **Credential Harvesting**, **Training**, **Vishing**, and **Smishing**.
78. This concludes the demonstration of auditing an organization's security for phishing attacks using OhPhish.
79. Close all the open windows and document all the acquired information.
80. Turn off the **Windows 10** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document all the results obtained in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE ANY QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs